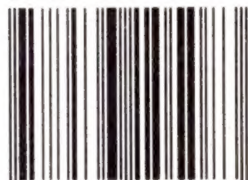
丢番图方程的计算方法

郭永东　薛国芬　李　由　编著

$$\left|\sum_{i=1}^{t} C_i \cdot \prod_{j=1}^{s_i} \alpha_{ij}^{n_{ij}}\right| < \min_i \left|C_i \cdot \prod_{j=1}^{s_i} \alpha_{ij}^{n_{ij}}\right|^{\delta}$$

新疆大学出版社

责任编辑：王少杰
封面设计：子　辛



ISBN7－5631－0508－5/O・5　定价：18.70元

丢番图方程的计算方法

郭永东　薛国芬　李　由

新疆大学出版社

(新)新登字08号

责任编辑:王少杰
封面设计:子　辛

丢番图方程的计算方法

郭永东
薛国芬　编著
李　由

出版发行:新疆大学出版社
(乌鲁木齐市胜利路14号　邮编:830046)
经　　销:新华书店
印　　刷:湛江恒辉彩色印刷有限公司
开　　本:850×1168毫米　1/32
印　　张:8.875
字　　数:191.3千字
版　　次:1995年12月第一版　1995年12月第1次印刷
印　　数:1－1000册

ISBN7－5631－0508－5/O·5　　定价:18.70元

序

丢番图方程的求解问题是数论研究中非常重要内容之一。近些年来，由于超越数论等出现了许多重要进展，为丢番图方程求解提供了重要和有效的工具，并形成了求解丢番图方程的近代方法，从而使得一大批丢番图方程获得有效的解决。

本书首先介绍了超越数论和丢番图逼近论中近年出现的著名Gelfond－Baker方法，L^3－算法等基本原理和方法。然后讲述这些方法在一些重要丢番图方程，如Thue方程，Thue－Mahler方程，S－单位方程，S－单位不等式等方面求解问题中的应用。该书既有有关理论的详细论述，又特别着重讲述这些理论如何具体实现几种类型方程的求解问题。这自然包括作者多年从事这一领域的研究成果和总结，同时本书提供的研究方法，可以应用到很多同类型的方程和逼近问题的解决，这对从事本领域研究和工作的同志有重要参考价值。本书也是国内首次介绍这一重要研究方向并有重要价值的一本书。

中国科学院
数学研究所
徐广善

内 容 简 介

丢番图方程是数论中的一个相当活跃的研究领域，本书系统地介绍了以 Baker 方法和 L^3 – 算法为基础的计算方法及其在丢番图方程中的应用．本书可供从事计算数论及其相关领域研究的数学工作者以及对此感兴趣的数学系大学生、研究生，中学数学教师和数论爱好者参考．

引　言

在数论中,通常将未知数个数多于方程或不等式个数,并且对未知数的取值加以某些限制(例如限制为整数、正整数等)的方程、方程组和不等式统称为丢番图方程.早在公元三世纪初,古希腊数学家 Diophantus 就已经对此类方程进行了比较系统的研究.我国最早的数学文献《周髀算经》也曾有过此类方程正整数解的记载.因此,丢番图方程是数论中最古老的分支.由于丢番图方程与数论、代数、组合数学等数学分支有着密切的联系,所以它一直是基础数学中的一个相当活跃的研究领域.

如果暂且不考虑不等式的情况,一般的丢番图方程都可以表成以下形式:

$$f(x_1, x_2, \cdots, x_m) = 0, \quad x_1, x_2, \cdots, x_m \in S,$$

其中 $f(x_1, x_2, \cdots, x_m)$ 是未知数 x_1、x_2、$\cdots$、x_m 的函数,S 是未知数取值的集合,该方程的求解就是要找出集合 S 中所有可使 $f(x_1, x_2, \cdots, x_m) = 0$ 成立的元素组 $(x_1, x_2, \cdots, x_m)$.具体来说,丢番图方程的种类异常繁多.Dickson 在他的名著《History of the Theory of Numbers》第二卷中,用了八百多页的篇幅也只能对本世纪初以前的工作给出了简要的介绍.但是从总体而言,迄今为止人们讨论较多的主要是以下两类方程.

当 $f(x_1, x_2, \cdots, x_m)$ 是 $x_1, x_2, \cdots, x_m$ 的整系数多项式时,

称为多项式方程．如果 $f(x_1, x_2, \cdots, x_m)$ 是 n 次多项式，则称它是 m 元 n 次方程．例如，著名的 Fermat 猜想就是要证明：当 n 是大于 2 的正整数时，三元 n 次方程

$$x^n + y^n = z^n, \quad x, y, z \in \mathbb{N}$$

无解 (x, y, z)．在一般情况下，元数越多，次数越高，则相应的多项式方程越不容易解决．

当 $f(x_1, x_2, \cdots, x_m)$ 是在指数位置上也有未知数的整系数多项式时，称为指数型方程．例如，至今尚未完全解决的 Catalan 猜想就是要证明：指数型方程

$$x^m - y^n = 1, x, y, m, n \in \mathbb{N}, x > 1, y > 1, m > 1, n > 1$$

仅有解 $(x, y, m, n) = (3, 2, 2, 3)$．

1900 年，Hilbert 在他的著名演讲中提出了二十三个重要的数学问题，这些问题直接影响着本世纪数学的发展．Hilbert 的第十问题提出：对于一般的整系数多项式 $f(x_1, x_2, \cdots, x_m)$，是否存在有限的算法来确定方程

$$f(x_1, x_2, \cdots, x_m) = 0, \quad x_1, x_2, \cdots, x_m \in \mathbb{Z}$$

的可解性？1970 年，Davis、Matijasevič 和 Robinson 运用数理逻辑方法否定地解决了这个问题，即证明了这样的有限算法是不存在的．上述结果说明了求解丢番图方程的困难程度．

近三十年来，由于 Baker 和 Lenstra 等人分别在超越数论和丢番图逼近方面的出色工作，对某些类型的丢番图方程已经有了求解的有限算法．目前，这些工作已经形成了数论中最年轻的分支——计算数论的主要内容．鉴于国内尚未见到这

方面的专门书籍，作者根据近年来学习丢番图方程的计算方法所取得的一点心得编写了本书，以供对此感兴趣的读者参考.

本书的前三章介绍了 Baker 方法、L^3－算法等基本方法的原理，后五章分别介绍了这些方法在 Thue 方程、Thue－Mahler 方程、S－单位方程以及 S－单位不等式等丢番图方程求解问题中的应用.

本书第一、二、五章由郭永东编写，第三、四、六章由薛国芬编写，第七、八章由李由编写. 全书由薛国芬、郭永东两人总纂.

乐茂华教授审阅了全书并作了一些修改和补充，作者表示感谢.

本书的写作和出版得到了国家自然科学基金和广东省自然科学基金的资助.

吴江先生对本书的出版给予热忱资助，作者深表谢意.

由于作者的水平所限，书中的误谬之处在所难免，切望读者不吝赐教.

作　　者

目　录

第一章　绪　论

1.1　丢番图方程的解法

本节论及丢番图方程的某些类型.通常将未知数个数多于方程或不等式个数,并且对未知数的取值加以某些限制(例如限制为整数,正整数等)的方程、方程组和不等式统称为丢番图方程.

例如本书将要研究的丢番图方程

$$x^2 + 7 = 2^n$$

(Ramanujan－Nagell 方程,恰有解$(\pm x, n) = (1,3),(3,4),(5,5),(11,7),(181,15)$,参见第四章);

$$2^x = 3^y + 5^z$$

(纯指数方程,恰有解$(x,y,z) = (1,0,0),(2,1,0),(3,1,1),(5,3,1),(7,1,3)$,参见第六章);

$$y^2 = x^3 - 4x + 1$$

(椭圆曲线方程,恰有 22 个解,其中最大的解是$(x,y) = (1274, \pm 45473)$,参见第八章).这里提及的三个方程仅是丢番图方程的一些例子.我们将研究更广泛类型的方程,我们也研究(在第五章)丢番图不等式(一个式子大于另一个式子的表达式,其解仍然限制为整数).在下面的讨论中,关于丢番图

方程的叙述也适用于丢番图不等式.

本书所论述的方程的共同点是它们都能用相同的方法求解.这种方法实质上由三部分组成:变换,Gelfond - Baker 理论的应用以及丢番图逼近.我们简扼地解释这些步骤.

首先,将方程变换成纯指数方程或不等式,即方程或不等式的未知数都出现在指数,例如上面列举的第二个例子.每一种类型的丢番图方程需用一种特别的变换,因此在此意义上更是特别困难.对于某些例子,象上述第二个例子,这种变换是容易的.另一方面的例子,如上面列举的第一个例子或第三个例子,可以运用代数数论的一些理论,这种例子是很多的.

这种纯指数方程的一般形式如下:

$$\sum_{i=1}^{t} c_i \cdot \prod_{j=1}^{s_i} \alpha_{ij}^{n_{ij}} = c_0 \cdot \prod_{j=1}^{s_0} \alpha_{0j}^{n_{0j}} \qquad (1\cdot1)$$

而对应的纯指数不等式形如

$$\left|\sum_{i=1}^{t} c_i \cdot \prod_{j=1}^{s_i} \alpha_{ij}^{n_{ij}}\right| < \min_i \left|c_i \cdot \prod_{j=1}^{s_i} \alpha_{ij}^{n_{ij}}\right|^{\delta} \qquad (1\cdot2)$$

其中,$t, s_i, c_i, \alpha_{ij}, \delta$ 是满足 $t, s_i \in N, 0 < \delta < 1$ 的常数,且 c_i, α_{ij} 属于 Q 的某代数扩张,n_{ij} 是 Z 中的未知数.现在我们假定(1·1)或(1·2)的左边的项数 t 等于 2.这一限制对于第二个步骤是必不可少的,因为我们要运用所谓代数数对数线性型理论的结果,也称为 Gelfond - Baker 理论(满足 $t > 2$ 的某些特殊类型的指数方程(1·1)也可用 Gelfond - Baker 方法来处理,因为他们可转化为满足 $t = 2$ 的形如(1·2)的指数不等式,有关这方面的详细情况可参阅文献[3]、[4]、[114]、[120]).

赋予满足 $t=2$ 的形如(1·1)或(1·2)的指数方程或不等式以对数线性型

$$\Lambda = \log\beta_0 + \sum_{i=1}^{m} n_i \cdot \log\beta_i$$

其中 β_i 是代数常数，n_i 是未知整数. 这里，对数在某些情况下是实数或复数，在其他情况下是 p－adic 数. 方程与对数线性型之间的这一关系使得方程的一个大解的线性型十分接近于零(在实的或复的情况下，或在 p－adic 情况下). Gelfond－Baker 理论提供了有效计算这种代数数的对数线性型的绝对值(特别是 p－adic 值)的下界的方法. 在许多情形下，这些界已确切计算出来. 把已找到的上界和下界作比较，就有可能得到指数丢番图方程或不等式的解的有效的上界，导出原来方程解的上界. 不象第一个步骤，这第二个步骤是相当一般自然的.

我们注意到，许多研究者已经应用上面概述的方法，给出了各种各样的丢番图方程解的有效的可计算的上界. 作为综述，请参看文献[107]. 这些研究者常常满足于知道这些上界的存在，而不实际求出这些上界. 如果他们求出这些上界，他们也不总是确定方程所有的解. 在本书中，解丢番图方程总是意味着：确切地求出方程所有的解.

在第二个步骤之后，解丢番图的问题就转化为一个有限问题，这由上述方法的第三个步骤来处理. 换句话说，因为我们已找到了未知数的绝对值的有效上界，我们就能检验未知数仅有的有限多种可能. 然而 Gelfond－Baker 理论提供的关于代数数对数线性型的下界中出现的常数相当大. 因此，实际

上用这种方法能得到的纯指数方程解的上界可以大得象常数10^{40}这么大. 上界太大以致不容许将所有可能完全列举，甚至用现今最快的计算机也做不到.

证明解的绝对值上界存在使得确定所有的解从无限问题归化为有限问题. 因此，Gelfond - Baker 理论的应用（第二个步骤）在一定意义上使无限多次的困难工作归化为进行有限多次的检验（第三个步骤）. 而且，这个检验几乎仅是技术问题而不是数学问题. 尽管如此，我们认为解决这个比较小的技术问题不仅是非平凡的，而且包含着重要和有趣的数学问题. 本书期待着举例证明这一见解.

尽管第二个步骤中 Gelfond - Baker 理论的应用实际上产生很大的上界，一般假定这些上界远非实际上的最大解. 因此，寻找将这些上界降低到容易处理的大小的方法是很值得研究的. 直接应用原来丢番图方程的某些性质来找出这种方法常常是可能的. 例如大数解必须满足多模或大数模的一定同余式（参见文献[26]、[45]、[96]），或满足某可逆性条件（参见文献[90]）. 这种方法的缺点是仅能用于特殊类型的丢番图方程，因此，一般情况下，对每一种类型的方程必须想出一种新的变换方法. 因此，对于对数线性型不等式的解降低上界的方法将是有趣的. 导出这样的不等式将可用于解每一类型的丢番图问题.

这种方法的研究是我们所述的解丢番图方程方法的第三个步骤. 在第三个步骤中，已发表的新的进展是主要的. 我们在第一、第二个步骤的讨论中应用的主要是经典的，我们将其应用于以前已研究过的各类型的方程，也用于一些新类型的方程.

第三个步骤需要提供的丢番图逼近理论的方法牵涉到研究如何能使给出变量的值的线性型接近零.在这方面近来已获得重要进展.惊人的进展是 1981 年 L·Lovász 创造了所谓 L^3 - 格基缩减运算.我们将阐明怎样由 L^3 - 运算导出实际有效的丢番图逼近运算,这种方法能用于证明许多丢番图方程在某个区间$[x_1, x_0]$上没有解存在.通常 x_1 是 $\log x_0$ 的数量级.当解被置换为理论的上界 x_0 时,通常一个新的更好的上界 x_1 就可以找到.对许多方程,这种运算的实际应用,仅在几分钟的计算机时之内便可得到初始上界 x_0.对于那些未找到变换的方法或变换未获成功的方程来说,上述导出了寻找许多类型的丢番图方程所有解的实际方法.

在本书中用于解许多例各种各样的丢番图方程的上述列举的方法,是一种"运算"特征.在一定意义上,它处于"特定的"方法与"理论的"方法之间.这一点我们将在下面解释.设给出带未指定参数的一个丢番图方程集合.作为这样的集合的一个例子,考虑广义 Ramanijan - Nagell 方程 $x^2 + D = 2^n$,其中 D 是一个参数,x、n 是未知数.

特定的方法是仅对参数的特殊值解方程的方法.它对这些特殊值以外的参数值不适用.解形如 $x^2 + D = 2^n$ 的方程的第一个例子出现在 Nagell1948 年的著作中,其中取 D = 7.他使用的方法是特定的特征,因为这种方法对参数 D 选取了特殊的固定值 7.

理论的方法可以对于参数值是某个大集合导出结果.Gelfond - Baker 理论是理论的特征,因为它对许多方程关于它们的参数导出解的上界.另一例子是平方互反性理论的应用,证明了若 D 是任意不小于 5 的奇数,则方程 $x^2 + D = 2^n$ 没

有解，且关于 7 不同余(mod 8)，而且，1981 年 Beukers[14]运用超几何函数理论证明了方程 $x^2+D=2^n$ 的解(x,n)满足 $n<435+10^2\cdot\log|D|$，而且若 $|D|<2^{96}$，则又有 $n<18+2^2\cdot\log|D|$. 理论的方法常常太一般以致不能导出给定方程的全部解.

计算的方法是保证对参数值的任一个集合都能进行的方法，但为了导出所有解，这是分别对参数值的每一个特殊集合来进行的. 在本书中应用的方法意味着这样一种计算的特征. 我们将在第 4 章中对方程 $x^2+D=2^n$(实际上是对更一般的方程)给出计算的方法. 事实上，由于 Beukers 的上述结果产生解的一个小上界，就能通过枚举所有解的简单方法来降低上界. 但是这一方法的计算部分是微不足道的，因此我们宁可将 Beukers 的方法归为理论上的一类. 为了进行 Gelfond - Baker 理论计算，枚举所有可能是不实用的. 因此，确定所有解的更巧妙方法是找到降低大上界的方法. 我们注意到 Beukers 方法对更一般方程 $x^2+D=p^n$ 也有其特定的方面，因为它仅对某一特殊的值 p 来考虑. 我们在第 4 章中的方法就没有这一缺点.

关于解丢番图方程的想法，可以努力的是设计一种计算机计算程序，一种“丢番图计算机”，仅需将方程的参数输入，短时间之后，所有解就列示出来. 我们理应保证(从严格的数学证明的意义说来)没有解被遗漏.

上述列举的方法乍看起来，在本书中叙述这样一种一般适用的解法似乎是较好的选择. 换句话说，在第二个步骤中，证明参数已确定的指数丢番图方程的上界，是一种十分一般的特征. 第三个步骤，计算丢番图逼近部分，就原理而论也可

用于参变量变换值的任一个集合，尽管计算是对每一个特殊值的集合分别进行的.

设计这样一种“丢番图计算机”的主要困难是上面列举的方法的第一个步骤，特别运用代数数论的某些理论的时候，在于代数数论的计算理论在计算单位元和找到素数的代数扩张的因子分解方面的形式，在这儿是很重要的. 我们认为，当这种相应的计算可得到时，那么设计出这种“丢番图计算机”原则上将是可能的(但在第三个步骤的技术困难不可低估)，这种计算多半限制在第一个步骤中的一般对数线性型变换. 本书仅在计算工作量大得有必要时才使用计算机计算，除此之外仍用“手工”操作. 采用这种方式，我们也力图使方法介绍得透彻.

读者应意识到这样的事实，计算机程序及其结果是我们的许多关于丢番图方程的定理的证明的一部分，但无论如何，这些程序和计算的全部细节不可能发表. 有兴趣的读者可通过程序设计者获得这些细节，并要求进行检验计算. Shorey 和 Tijdeman 的著作[107]对于能够运用 Gelfond－Baker 方法求出上界从而找到解的丢番图方程作了详细的综述. 某些这样的方程用本节叙述的方法可以完全解出，它们有纯指数方程，含二元递归序列的方程，Thue 方程和 Thue－Mahler 方程. 特别是后两种方程在数论的各个其他部分是重要的. 例如他们是解 Mordell 方程以及产生于代数数论和计算代数几何的各种各样方程的关键. Gelfond－Baker 方法首次实际被用于解丢番图方程是 Baker 和 Davenport 在 1969 年的工作，他们用于解丢番图方程组

$$3 \cdot x^2 - 2 = y^2, \qquad 8 \cdot x^2 - 7 = z^2$$

出现在文献中的能计算解的上界的其他方程用我们的计算方法难以处理，因为对这些方程来说，对数代数线性型理论的应用更难弄，况且其上界实质上太大.这种方程的一个例子是 Catalan 方程 $a^x - b^y = 1$，其中 a、b、x、y 都是大于或等于 2 的整数.Catalan 在 1844 年曾猜想此方程仅有解 $(a, b, x, y) = (3, 2, 2, 3)$.1976 年，Tijdeman[117]证明了 Catalan 方程的解以一个可计算的数为界，根据 Langevin[61]，这个数可以取为 $\exp(\exp(\exp(730)))$.然而，我们未能看到如何应用我们在后面各章所叙述的方法找到 Catalan 方程的全部解.

另一个好几世纪以来引起广大数学工作者注意的丢番图方程是 Fermat 方程 $x^n + y^n = z^n$，其中 x、y、z、n 是满足 $n \geqslant 3$ 且 $xyz \neq 0$ 的整数.已猜想此方程无解.Faltings[41]证明了对固定的 n 此方程的解数是有限的，他的证明是无效的.Gelfond-Baker 理论看起来似乎不足以处理充分一般的 Fermat 方程，甚至当 n 是固定的情况.运用这一理论已获得的关于 Fermat 方程的部分结果的综述可参阅 Tijdeman[118]以及 Shorey 和 Tijdeman[107]第 11 章.最近，这个问题已被 Wiles 运用代数几何方法解决了.

我们注意到关于许多丢番图方程新近的重要进展建立在对解的个数确定上界.有关这方面的详细情况可参见文献[39]、[40]、[66]、[103].这些结果往往是明显值得注意的，但却是非实效的，因为他们不能用来实际找出解.

作为本节的结束，我们给出本书内容的一个概述.本书分为三部分：第 1 章是绪论，第 2、3 章给出必要的准备工作，第

4到第8章论及各种各样类型的丢番图方程.

第1·2至1·5节分别对非特殊的Gelfond－Baker理论,丢番图逼近理论,丢番图逼近的计算以及降低上界的程序给出简短的导论.第二章包括我们所需的来自代数数论与p－adic数及其函数理论的初步结果,并从我们运用的Gelfond－Baker理论中引论充分详细的定理,它以一些数值方法的陈述为结束.第3章详细给出我们在后面各章中应用的丢番图逼近理论方面的计算.在一定意义上这一章是本书的中心.

第4章到第8章,每一章致力于一定类型的丢番图方程.设$p_1,\cdots,p_s$是不同素数的一个固定集合.设S是仅由素数$p_1,\cdots,p_s$组成的正整数集合.

第4章论及S中的二元递归序列("广义Fibonacci序列")的元素,并应用于各式各样的二次指数方程,例如广义的Ramanujan－Nagell方程$x^2+k\in S$(其中k固定).本节的丢番图逼近部分是有趣的,理由有二:p－adic逼近非常简单,且在递归有负求解的情况下,p－adic和实的或复的逼近理论发生了深刻的联系.第4章的研究分别是由Pethö和de Weger[93] de Weger[135]完成的.

第5章论及丢番图不等式$0<x-y<y^\delta$,其中$x,y\in S$,并指定$\delta\in(0,1)$.第6章论及方程$x+y=z$,其中$x,y,z\in S$,这可考虑作为第5章中的不等式的p－adic模拟.这两种方程是能用我们的方法处理的丢番图方程的最简单例子.因为他们已经是形如(1·1)或(1·2)满足$t=2$的纯指数方程,其解法第一步骤是微不足道的:对数线性型正好与方程有关.因此,他们适宜作为对我们的方法中丢番图逼近部分得到明白了解的好例子.这两章的结果可参见文献[136].

在第七章，研究方程 $x+y=z^2$，其中 $x, y \in S, z \in Z$. 这方程是第4章中研究的广义 Ramanujan－Nagell 方程的进一步推广.

在第8章，给出解 Thus 方程的一个程序，这一工作就原理而论适合任意次数的 Thus 方程. 它被应用于寻找椭圆曲线方程 $y^2=x^3-4x+1$ 的所有整数点. 我们也简短地叙述怎样的 Thus－Mahler 方程能用此类方法解决. 有关这方面的详细情况可参见文献[124]、[138].

1·2 Gelfond－Baker 方法

在第1·1节中，我们已经解释了对某些方程应用 Gelfond－Baker 方法之前必须将方程变换成项数不太多的纯指数方程或不等式（参阅(1·1)，(1·2)）. 在这一节我们概略讨论用 Gelfond－Baker 理论对这种指数方程或不等式的变量导出上界.

首先让我们处理不等式(1·2)的情形. 由于 $t=2$，我们可假定它有如下形式：

$$\left|\alpha_0 \prod_{i=1}^{s} \alpha_i^{n_i} - 1\right| < c_0 \cdot \exp(-\delta \cdot N)$$

其中 α_i 是固定的代数数，$N=\max|n_i|$，且 c_0，δ 是正常数. 在我们研究的例子中，我们遇到了下面两种情况之一：或者所有 α_i 是实的，或者对所有 i，$|\alpha_i|=1$. 在实的情况下，若 N 足够大，则对数线性型

$$|\Lambda| = \log|\alpha_0| + \sum_{i=1}^{s} n_i \cdot \log|\alpha_i|$$

必须满足对某个 c_0'

$$|\Lambda| < c_0' \cdot \exp(-\delta \cdot N) \qquad (1\cdot 3)$$

成立.在复的情况下,相同的不等式(1·3)由线性型

$$\Lambda = \log\alpha_0 + \sum_{i=1}^{s} n_i \cdot \log\alpha_i + k \cdot \log(-1)$$
$$= i \cdot [\mathrm{Arg}\alpha_0 + \sum_{i=1}^{s} n_i \cdot \mathrm{Arg}\alpha_i + k\pi]$$

导出,其中对数及反对数函数取其主值.现在我们可以从 Gelfond－Baker 理论的许多结果中得到应用,给出 $|\Lambda|$ 关于 N 的一个确切的下界.例如下面定理.

定理 1·1 (Baker[9]) 设 Λ 如上面所列示.存在仅依赖于 α_i 的可计算常数 c_1, c_2,使得若 $\Lambda \neq 0$,则

$$|\Lambda| > \exp[-(c_1 + c_2 \cdot \log N)]$$

我们通常已知 $\Lambda \neq 0$.结合(1·3)及定理 1·1,得

$$N < \frac{c_1 + \log c_0'}{\delta} + \frac{c_2}{\delta} \cdot \log N$$

由上述导出 N 是界.

其次考虑指数方程(1·1).由于 $t=2$,我们可将其写成

$$\alpha_0 \cdot \prod_{i=1}^{s} \alpha_i^{n_i} - 1 = \beta_0 \cdot \prod_{j=1}^{r} \beta_j^{m_j}$$

其中 α_i, β_j 是固定的代数数. 设 H_p 是 $|n_i|, |m_j|$ 的极大值, 其中 i, j 跑遍与 α_i 相应的下标集合. β_i 是非基数. 设 H 是 $|n_i|, |m_j|$ 的极大值, 其中 i, j 跑遍所有下标集. 假定 p 是关于某些 j 落在 β_j 上的一个有理素数. 存在常数 c_1, c_2, 使得

$$\mathrm{ord}_p[\alpha_0 \cdot \prod_{i=1}^{s} \alpha_i^{n_i} - 1] \geqslant c_1 + c_2 \cdot m_j.$$

假定对所有 i, $\mathrm{ord}_p(\alpha_i) = 0$, 我们可以写出下面的 p - adic 对数线性型

$$\Lambda = \log_p \alpha_0 + \sum_{i=1}^{s} n_i \cdot \log_p \alpha_i,$$

由此, 若 m_j 足够大, 便可导出

$$\mathrm{ord}_p(\Lambda) \geqslant c_1 + c_2 \cdot m_j \qquad (1 \cdot 4)$$

现在, 我们能够应用从 p - adic Gelfond - Baker 理论导出的下面结果. 这儿, $N = \max |n_i|$.

定理 1·2(Van der Poorten[98], 于坤瑞[141])设 Λ, p 如上. 存在仅依赖于 α_i 和 p 的可计算常数 c_3, c_4, 使得若 $\Lambda \neq 0$, 则

$$\mathrm{ord}_p(\Lambda) < c_3 + c_4 \cdot \log N.$$

对所有可能的 p 应用(1·4)和定理 1·2, 我们得到常数 c_3',

c_4',满足

$$H_p < c_3' + c_4' \cdot \log H.$$

若对某常数 c_5, $H \leqslant c_5 \cdot H_p$,则直接得到关于 H 的一个上界.若 $H > c_5 \cdot H_p$,则可证明存在 α_i, β_i 的一对共轭值,用加“′”的符号表示,使

$$\left| \beta_0' \cdot \prod_{j=1}^{r} \beta_j'^{m_j} \right| < \exp(-c_6 \cdot h)$$

对常数 c_6 成立(参阅文献[107]PP.45-49 定理 1·4 的证明).现在我们可以应用定理 1·1 导出

$$\left| \alpha_0' \cdot \prod_{j=1}^{s} \alpha_j'^{n_j} - 1 \right| > \exp[-(c_7 + c_8 \cdot \log H)].$$

由上式导出 H 是界.

若碰巧 α_i, β_i 没有一个是基数,则当然足以应用定理 1·2.

我们注意到,为了能完全地解丢番图方程,关键是所有常数可清楚的计算.因此,我们仅能运用由 Gelfond-Baker 理论能够完全显示的界.我们在 2·4 节详细给出这样的定理.

1·3 理论的丢番图逼近

在本节我们简洁地叙述丢番图逼近理论的一些结果,为下节作些准备,更详细的叙述可参考文献[30],[59],[53],[102],[104].

在实的情形下,丢番图逼近最简单的形式是用有理数p/q

逼近一个实数 θ, 众所周知, 若 θ 是无理数, 则丢番图不等式

$$\left|\theta-\frac{p}{q}\right|<q^{-2}$$

存在满足 $(p,q)=1$ 的无限多个解 $(p,q)\in Z\times N$, 由 θ 的连分数展开式得到的所有渐近分数是这样的解. 对任意特殊的 $\theta\in R$, 渐近分数的计算是简单的.

一种一般化的途径是研究同步逼近一个实数集合 $\theta_1,\cdots,\theta_n$, 即所有有相同分母的有理逼近于 θ_i. 如所熟知, 若 θ_i 中最小的一个是无理数, 则不等式组

$$\left|\theta_i-\frac{p_i}{q}\right|<q^{-(1+1/n)},\quad i=1,\cdots,n$$

有无限多个解 $(p_1,\cdots,p_n,q)$. 但求出这样的不等式的解要比 $n=1$ 的情况困难得多. 一些多维的连分数计算已经作出(参阅文献[25]综述部分), 但他们似乎不考虑简单化和一般化. 后面将看到, 我们就此问题如何应用所谓 L^3 - 算法.

丢番图逼近最简单情形的另一种一般化途径是研究线性形, 有如

$$L=\sum_{j=1}^{m}q_j\cdot\theta_j$$

其中 $\theta_1,\cdots,\theta_m$ 是给定实数, $q_1,\cdots q_m$ 是 Z 中的未知数. 设 $Q=\max|q_j|$, 一个经典的定理保证了不等式

$$|L-p|<Q^{-m}$$

存在一个解 $(p,q_1,\cdots,q_m)$.

注意 $m=1$ 的情形, 此不等式两边除以 $q=q_1$, 就变成第

一个不等式. 在此情形下, 正如我们下面将看到的, L^3 - 算法也是非常有效的.

我们能将上述两种一般化的途径归并为更一般的结果, 即线性型的同步逼近. 设实数 θ_{ij} 已给出, 其中 $i=1,\cdots,n,j=1,\cdots,m$, 令

$$L_i=\sum_{j=1}^{m}q_j\cdot\theta_{ij},\quad i=1,\cdots,n$$

依关于 Minkowski 条件的一个著名定理, 不等式组

$$|L_i-P_i|<Q^{-m/n},\quad i=1,\cdots,n$$

存在一个解 $(p_1,\cdots p_n,q_1,\cdots,q_m)$.

正如我们将在 1·4 节看到的, L^3 - 算法可用于这种一般型. 若右边是大于 1 的一个小常数的倍数, 则实际计算此不等式组的解稍为容易些.

现在我们考虑非齐次逼近. 这意味着对所有 i, 在线性型 L_i 中存在非齐次项 β_i, 即

$$L_i=\beta_i+\sum_{j=1}^{m}q_j\cdot\theta_{ij},\quad i=1,\cdots,n$$

同时, 存在一个常数 c, 使不等式组

$$|L_i-p_i|<c\cdot Q^{-m/n},\quad i=1,\cdots,n$$

在关于 β_i 和 θ_{ij} 的某无关条件下有一个解. 这就是 Kronecker 的定理. m = n = 1 的最简单情况下, 变成

$$|q\cdot\theta-p+\beta|<c\cdot q^{-1}$$

上面给出的上界告诉我们，$|L_i-p_i|$的数量级最小如$Q^{-m/n}$那么小，而非仅是理论上的上界，但他们同样预示探试的期望数量级. 由此，我们意识到在一般情况下(即当θ_{ij}(或β_i)之间不存在准线性关系时)，实际情形是对给定的Q_0，最小的$\max_i|L_i-p_i|$，取代所有$Q\leqslant Q_0$，有上界$Q^{-m/n}$的数量级.

为结束本节，我们注意到，存在着这一丢番图逼近理论的p-adic模拟，由Makler和Luts发现. 若我们用Q_p代替上面考虑的R，用p-adic值$|\cdot|_p$代替绝对值$|\cdot|$，用R^{n+m}上任意的凸范数$\varphi(p_1,\cdots p_n,q_1,\cdots,q_m)$代替关于逼近$(p_1,\cdots p_n,q_1,\cdots,q_m)$的量值Q，则Minkowski和Kronecker的p-adic模拟定理实质上是对上述结果在实的情形的模拟. 关于Mahler的工作可参考文献[59]、[71]、[134].

1·4 计算的丢番图逼近

本节给出解丢番图方程遇到的实用的解丢番图逼近问题的一些思想. 在本节我们不作严格论述，我们忽略最不利的情形，而集中于怎样做预期的工作(根据1·3节的探试)，且可视为实际的工作. 后面各章给出的许多例子表明我们的方法事实上是真正有效的. 实际上应用此方法是获得必要的有限逼近方法的最好方式.

我们将论及下面计算的丢番图逼近问题. 设给定$\theta_{ij},\beta_i\in R$，$p_1,\cdots p_n,q_1,\cdots,q_m$是未知整数，满足$Q=\max|q_i|$. 设$L_i$如

上述．假定正常数 Q_0 是已给定的一个相当大的数，比如 10^{50}．寻求关于值

$$\max_i |L_i - p_i|$$

的一个下界，其中$(p_1, \cdots p_n, q_1, \cdots, q_m)$跑遍满足 $Q \leqslant Q_0$ 的值集．从 1·3 节探求要点可导出，若这个下界的大小是 $Q_0^{-m/n}$，则必能被满足．对 p－adic 情形，模拟问题可以公式化．

与丢番图逼近理论相关的问题是对于固定的 $\varepsilon > 0$，实际找到$\max_i |L_i - p_i| < \varepsilon$ 的一个有效解或最大解．正如我们将要看到的，L^3－算法是找到有效解的很有用的工具．无论如何，寻找最大解的问题本质上似乎是更困难．我们注意到，在多数情况下，我们解丢番图方程所运用的，是对给定的 Q_0，取得关于$\mathrm{mac}_i |L_i - p_i|$的合适的下界就足够了，而不必要确切地知道这个下界是怎样显示的．

我们解前述问题所用的计算工具是所谓 L^3－格基缩减运算，叙述在 Lenstra, Lenstra 和 Lovóse[69]．我们将在 3·4 和 3·5 节给出这种运算的详细叙述．下面我们简短地指出其怎样能运用于解丢番图逼近问题．

设 Γ 是 R^n 中的格，L^3－运算允许 Γ 中的任意基 $\underline{b}_1, \cdots, \underline{b}_n$ 作为输入．作为输出，给出相同格 Γ 的另一个基 $\underline{c}_1, \cdots, \underline{c}_n$，那就是所谓简化基，简化的概念意味着大约接近于正交．用简化基就有可能计算下面两个量的下界：

→最接近原点的非零格点的距离

$$l(\Gamma) = \min_{\underline{0} \neq \underline{x} \in \Gamma} |\underline{x}|$$

(参考文献[69]的命题(1·11)，本书的引理 3·4)

→对任意给定点 $\underline{y}\in R^n$，从 $\underline{y}$ 到最近的格点的距离：

$$l(\Gamma,\underline{y})=\min_{\underline{x}\in\Gamma}|\underline{x}-\underline{y}|$$

(参考文献[5]以及本书的引理 3·5 和 3·6).

L^3 - 运算享有的性质是这些下界通常接近实际的最小解. 在一种生成状态，其格不太改变，简化基的向量 $\underline{c}_i$ 都有大约相同的距离，其数量级是

$$\det(\Gamma)^{1/n}$$

$l(\Gamma)$的值以及对其计算出的下界差不多一样大. 若 $\underline{y}$ 不太接近于一个格点，对 $l(\Gamma,\underline{y})$同样有效. 此外，在理论意义和实际上(参阅文献[68]P.7)计算的运行时间都是适宜的.

为了解决上述寻找关于$\max_i|L_i-p_i|$的下界问题，我们取格 Γ 如下. 设 c 是一个整数，至少象 $Q^{1+m/n}$那么大. n + m 维的格 Γ 用特定的基即矩阵

$$B=\begin{bmatrix} 1 & & & & & \\ & \ddots & & & \varnothing & \\ \varnothing & & 1 & & & \\ [C\cdot\theta_{11}] & \cdots & [C\cdot\theta_{1m}] & -C & & \\ \vdots & & & & \ddots & \\ [C\cdot\theta_{n1}] & \cdots & [C\cdot\theta_{nm}] & \varnothing & & -C \end{bmatrix}$$

的列向量 $\underline{b}_1,\cdots,\underline{b}_{n+m}$来定义(符号∅意味着所有没有明确给出值的范围都是零). 对这个格运用 L^3 - 运算我们找到一个简化基，其基向量将大约有距离 $C^{n/(n+m)}$，其大小近似于 Q_0. 一般地说，C 较大，简化基的基向量距离也较大(且关于 $l(\Gamma)$

和 $l(\Gamma, \underline{y})$的下界也较大).

让我们首先讨论齐次的情形，即对所有 $i, \beta_i = 0$，考虑格点 $\underline{x} = B \cdot [q_1, \cdots, q_m, p_1, \cdots, p_n]^T$. 它等于

$$\underline{x} = [q_1, \cdots, q_m, \widetilde{L}_1 - C \cdot p_1, \cdots, \widetilde{L}_n - C \cdot p_n]^T,$$

其中

$$\widetilde{L}_i = \sum_{j=1}^{m} q_j \cdot [C \cdot \theta_{ij}], \quad i = 1, \cdots, n.$$

应用 L^3－运算，我们找到关于 $l(\Gamma)$的一个下界，其大小为 Q_0. 我们假定它足够大(若非如此，我们尝试关于 C 的稍为大些的值，并再一次对被这个 C 限定的格进行 L^3－运算). 这样，我们可假定存在一个较小的常数 C_1，使得

$$\sum_{i=1}^{n} (\widetilde{L}_i - C \cdot p_i)^2 \geqslant l(\Gamma)^2 - m \cdot Q_0^2 > C_1 \cdot Q_0^2.$$

我们有 $|\widetilde{L}_i - C \cdot L_i| \leqslant m \cdot Q_0$，因此我们可假定对较小的常数 C_2, C_3

$$\max_i |L_i - p_i| > C_2 \cdot C^{-1} \cdot \max |\widetilde{L}_i - C \cdot p_i| > C_3 \cdot Q_0 / C.$$

由 C 的选择，这个最后的界大小合符要求.

其次，我们研究非齐次的情形，这里 β_i 不全为零. 我们如同齐次的情形取相同的格 Γ(注意格的定义仅依赖于 θ_{ij} 和 C)，考虑点

$$y = [0, \cdots, 0, -[C\cdot\beta_1], \cdots, -[C\cdot\beta_n]]^T,$$

由 L^3 - 运算，从简化基我们找到关于 $l(\Gamma, y)$ 的一个下界. 假定其足够大，大小为 Q_0. 我们如同齐次的情形取相同的格点 $x = B\cdot[q_1, \cdots, q_m, p_1, \cdots, p_n]^T$，则

$$x - y = [q_1, \cdots, q_m, \tilde{L}_1 - C\cdot p_1, \cdots, \tilde{L}_n - C\cdot p_n]^T,$$

其中

$$\tilde{L}_i = [C\cdot\beta_i] + \sum_{j=1}^{m} q_j\cdot[C\cdot\theta_{ij}], \quad i = 1, \cdots, n$$

与齐次的情形理由相同，现在导出需要的结果. 注意到若我们对给定的 θ_{ij} 已进行了一些 L^3 - 运算，我们可运用其结果处理齐次的情形，一样可以处理具有不同 β_i 的许多非齐次情形，只要 θ_{ij} 是相同的.

先前叙述如何求丢番图不等式组的下界. 由上述可清楚看到，求有效解是不困难的，即满足 $Q \leqslant Q_0$ 及 $\max_i |L_i - p_i|$ 的 $(q_1, \cdots, q_m, p_1, \cdots, p_n)$ 接近于最可能的值. 事实上，在齐次的情形，简化基的基向量是满足要求的，而在非齐次的情形，接近 y 的格点是这样的解. 接近 y 的格点不难一次找到一个简化基是合用的. 特别地，若 $s_1, \cdots, s_n \in R$ 是 y 关于简化基的坐标，则可取（关于简化基）坐标 $t_i \in Z$ 的格点趋于 s_i, $i = 1, \cdots, n$.

上述定义的矩阵中出现表达式 $[C\cdot\theta_{ij}]$，利用这一表达式我们构造了一个完全整数的格，即 $\Gamma \in Z$. L^3 - 运算能确切地适合于这些格，因此偏离的错误就可避免（参阅 3·5 节）. 错误

仅在 $\tilde{L}_i$ 和 $C\cdot L_i$ 两者不相同时才会发生，因此，通过选择适当的常数 C_1, C_2, C_3 可保持在控制之下．当然我们必须精心取 θ_{ij} 和 β_i 的数值精确到充分的精度．我们在 2·5 节简短地讨论这一数值问题．

上述丢番图逼近问题的可变更方法是对线性型 L_i 给予加权，即对

$$\max w_i|L_i - p_i|$$

寻找下界，这里 w_i 是固定正数．这种情况，通过用 $C\cdot w_i$ 代替矩阵第 $(n+i)$ 行的每一个 C，是易于处理的．

另一个变更方法是此处并非所有变量 q_j 都有相同上界 Q_0 的问题．为着说明这一点，假定 $n=1$，且

$$L = \sum_{j=1}^{m} q_j \cdot \theta_j$$

现在假定对某 $Q_1 > Q_2$（须便于使 $Q_2 | Q_1$），我们感兴趣的是满足

$$|q_j| \leqslant Q_1，当\ j \leqslant m_1；\quad |q_j| \leqslant Q_2，当\ j \geqslant m_1+1$$

的解．

其次设 C 的大小是

$$Q_1^{m_1+1} \cdot Q^{m-m_1}$$

并取矩阵

$$\begin{bmatrix} 1 & & & & & & \\ & \ddots & & & \varnothing & & \\ & & 1 & & & & \\ & \varnothing & & Q_1/Q_2 & & & \\ & & & & \ddots & & \\ & & & & & Q_1/Q_2 & \\ [C\cdot\theta_1] & \cdots & [C\cdot\theta_{m_1}] & [C\cdot\theta_{m_1+1}] & \cdots & [C\cdot\theta_m] & -C \end{bmatrix}$$

其行列式的大小是 Q_1^{m+1}. 对格点$[q_1,\cdots,q_m,\widetilde{L}-C\cdot p]^T$, 我们因此期望 $\max(|q_1|,\cdots,|q_{m_1}|)$, $(Q_1/Q_2)\cdot\max(|q_{m_1+1}|,\cdots,|q_m|)$和$|\widetilde{L}-C\cdot p|$的大小都是 Q_1. 由此导出$|L-p|$的大小是 $Q_1^{-m_1}\cdot Q_2^{-(m-m_1)}$. 这一变换对于应用实的和 p-adic 的方法的结合是有用的, 这有如 Thue-Mahler 方程(看 8·6 节).

我们通过给出 p-adic 丢番图逼近的模拟方法来结束这一节. 我们假定 $\theta_{ij},\beta_i\in Q_p$, 此外, 他们是 p-adic 整数. 设 $N_0=N\cup(0)$, 对任意 p-adic 整数 γ 和任意 $\mu\in N_0$, 我们用 $\gamma^{(\mu)}$表示唯一的有理整数, 使得

$$\gamma\equiv\gamma^{(\mu)}(\bmod p^\mu), \qquad 0\leqslant\gamma^{(\mu)}<p^\mu.$$

设 $\mu\in N$ 使得 p^μ 大致上如同 $Q_0^{1+m/n}$ 一样大小, 又假定 μ 足够大(它是常数 C 在上述实的情形的模拟)取格 Γ 使其基由矩阵

$$
B=\begin{bmatrix}
1 & & & & & \\
 & \ddots & & & \varnothing & \\
\varnothing & & 1 & & & \\
\theta_{11}^{(\mu)} & \cdots & \theta_{1m}^{(\mu)} & p^{\mu} & & \\
\cdots & \cdots & \cdots & \cdots & \cdots & \\
\theta_{n1}^{(\mu)} & \cdots & \theta_{nm}^{(\mu)} & \varnothing & & p^{\mu}
\end{bmatrix},
$$

的列向量给出. 考虑格点

$$B\cdot[q_1,\cdots,q_m,z_1,\cdots,z_n]^T=[q_1,\cdots,q_m,p_1,\cdots,p_n]^T.$$

则显然有

$$p_i=\sum_{j=1}^{m}q_j\cdot\theta_{ij}^{(\mu)}+z_ip^{\mu}$$

因此,格 Γ 被表示为集合

$$\Gamma=\{[q_1,\cdots,q_m,p_1,\cdots,p_n]^T\in Z^{m+n}\mid\sum_{j=1}^{m}q_j\cdot\theta_{ij}\equiv p_i \pmod{p^{\mu}},i=1,\cdots,n\}$$

L^3－运算提供关于此集合的非零向量的长度的一个下界,其大小与 $p^{\mu\cdot n/(n+m)}$ 相同,且属于 Q_0. 只要 μ 取得足够大,便可导出所需的结果.

对于非齐次的情形,设

$$\underline{y}=[0,\cdots,0,-\beta_1^{(\mu)},\cdots,-\beta_n^{(\mu)}]^T,$$

考虑集合

$$\Gamma^* = \{[q_1, \cdots, q_m, p_1, \cdots, p_n]^T \in Z^{n+m} \mid \beta_i + \sum_{j=1}^{m} q_j \cdot \theta_{ij} \equiv p_i (\mathrm{mod}\ p^\mu), i = 1, \cdots, n\}$$

当且仅当 $\underline{x} + \underline{y} \in \Gamma$ 时，有 $\underline{x} \in \Gamma^*$，因此 Γ^* 是一个变换格. 对于 $l(\Gamma, \underline{y})$ 的下界便导出所需的结果.

如同实的情形，再变换是可能的，例如在第$(n+i)$行用不同的 μ_i 代替 μ. 用这种方法甚至可能同时处理多个素数 p，只要在第$(n+i)$行用不同的 $p_i^{\mu_i}$ 代替 p^μ.

我们对 p－adic 情形再简述一个变换. 假定我们仅有一个线性型 $\Lambda = \sum_{j=1}^{m} q_j \cdot \theta_j$，一个参变量 $p \in Z$，我们要研究何时 Λ 与 0 同余，模是不同素数幂 $p_1^{\mu_1}, \cdots, p_n^{\mu_n}$. 因此，我们感兴趣的是集合

$$\Gamma' = \{[q_1, \cdots, q_m, p]^T \in Z^{m+1} \mid \sum_{j=1}^{m} q_j \cdot \theta_j \equiv p (\mathrm{mod}\ p_i^{\mu_i}), i = 1, \cdots, n\}$$

因此，对所有 j，取 $\theta_j^* \in Z$，满足

$$\theta_j^* \equiv \theta_j \quad (\mathrm{mod}\ p_i^{\mu_i}), \quad i = 1, \cdots, n,$$

$$0 \leqslant \theta_j^* < \prod_{i=1}^{n} p_i^{\mu_i},$$

θ_j^* 可用中国剩余定理计算. 现在，Γ' 便是由

$$\begin{bmatrix} 1 & & & \\ & \ddots & \varnothing & \\ & \varnothing & 1 & \\ \theta_1^* & \cdots & \theta_m^* & \prod_{i=1}^{m} p_i^{\mu_i} \end{bmatrix}$$

的列向量生成的格，而且从这个格，可按上面所述的继续进行下去.

我们用三点附注来结束本节. 首先考虑格的维数仅为 2 的情形，其 L^3 – 运算本质上是连分数运算，故得不到任何新的东西. 对 p – adic 连分数运算，参阅文献[134]. 其次，实线性型的丢番图逼近的非齐次情形也可用已知的 Davenport 引理来处理，可参阅文献[11]以及[36]. 我们将在第 3 章回到这个问题上来，并说明我们为什么更喜欢我们的方法.

最后，特殊的丢番图逼近的上述方法的一个优美特征是若一个最大解存在，则在齐次的情形，其格(具有适当常数 C 和 μ)将变形. 这意味着简化基将不象预期的那么优美. 例如，可能存在一个基向量大体上较其他的短. 在非齐次情形，最大解存在意味着存在一个格点极端接近于 $\underline{y}$. 运算立即看出这种反常状态. 在多数情形，其最大解都显示给出(例如，在齐次情形，如同简化基向量). 可以检验，此处这个最大解实际上满足原来的方程. 接着做下去，用除了最大一个之外的所有格向量的下界代替以上推理 $l(\Gamma)$ 或 $l(\Gamma, \underline{y})$. 这些新下界一般就是所期待的大小. 然而，我们实际解丢番图方程时从不会遇到这种反常状态.

1·5 降低上界的程序

在 1·2 节我们已看到，怎样找到指数不等式或方程存在的解的上界. 在 1·4 节我们研究了从估计的特殊点进行丢番图逼近的理论. 现在，将两者结合起来.

对 Gelfond－Baker 理论的应用，我们从以下问题出发. 我们有线性型

$$\Lambda=\beta+\sum_{j=1}^{m}n_j\cdot\theta_j$$

此处 β 和 θ_j 是常数(他们是代数数对数现在并不重要)，n_j 是未知整数. 我们知道，Λ 极靠近于 0，即

$$|\Lambda|<C\cdot\exp(-\delta\cdot N),$$

其中 C,δ 是(小)常数，$N=\max|n_j|$. 最后，我们得到关于 N 的显示的上界 N_0. 这个 N_0 非常大，比如 10^{50}.

我们已清楚，用 1·4 节中概述的方法来解决这个问题. 对于 Q_0，取 N_0，我们有 $n=1$，在实的情形，我们要求选择 C 的大小最低限度是 N_0^{m+1}，则对于小常数 C'

$$|\Lambda|>C'\cdot N_0^{-m}.$$

结合关于$|\Lambda|$的两个不等式，得到

$$N<\log(C/C')/\delta+(m/\delta)\cdot\log N_0.$$

因此 N 的上界 N_0 被降低到上界 N_1，其大小是 $\log N_0$，这的确

是不可忽视的改进．现在，我们用 N_1 取代 N_0，并按此过程重复做下去，直至得不到进一步的改进为止．实际上几乎经常出现的情况是降低了的上界接近于实际的最大解．无论如何，在满足需要的界之下寻找所有解的简单方法是微不足道的．

在 p－adic 情形，模拟的降低上界也能达到．相似的理由如下．由线性型 Λ（参看(1·4)式），我们有

$$\mathrm{ord}_p(\Lambda) \geqslant C_1 + C_2 \cdot m_j,$$

其中 C_1, C_2 是小常数，m_j 是变量，此外，变量以大常数 N_0 为界，这是显然的．取 μ 使得 p^μ 的大小至少是 N_0^{m+1}，因此，关于 Γ（或 Γ^*）中最短的非零向量的下界比 $\sqrt{m \cdot N_0}$ 大．由此导出格 Γ（或变换格 Γ^*）的元素不是(1·2)的解．因此，

$$C_1 + C_2 \cdot m_j < \mu.$$

因此，我们找到了关于 m_j 的一个新上界，其大小是 μ，大约是 $\log N_0/\log p$．为了得到关于 H_p 的降低的上界，我们对所有 m_j 重复这一过程．若这仍然不足以立即得到降低了的关于 H 的上界，则我们可以对实线性型应用简化步骤，以便于对某些变量刚好找到好得多的上界（参阅 1·4 节中第二种变更方法）．我们尽可能再重复全部程序．

第二章　代数数论与超越数论

2·1　代数数论

本节引进代数数论的一些结果，这些结果的运用贯穿在以后各章之中.这些结果的详细证明可参见文献[21]、[42]、[89].

设 K 是 Q 的次数 D＝[K:Q]的有限代数扩张.此时存在 D 个嵌入 $\sigma: K \to C$.设 $\alpha \in K$ 是次数为 d 的元素，并设 $a_0>0$ 是 Z 上 α 的最小多项式的首项系数.我们定义 α 的 Weil 高 $h(\alpha)$ 为

$$h(\alpha)=\frac{1}{D}\cdot\log[a_0^{D/d}\cdot\prod_{\sigma}\max(1,|\sigma(\alpha)|)],$$

其中，乘积 $\prod_{\sigma}$ 取遍所有嵌入 σ.由于这一定义不依赖于域 K.因此，若 α 的共轭数是 $\alpha=\alpha_1,\cdots,\alpha_d$，则对 $K=Q(\alpha)$ 应用上述定义，可得

$$h(\alpha)=\frac{1}{d}\cdot\log[a_0\cdot\prod_{i=1}^{d}\max(1,|\sigma_i|)].$$

特别是当 $\alpha\in Q$ 时，如果 $\alpha=q/g$，$(p,q)=1$，$p,q\in Z$，则必有 $h(\alpha)=\log\max(|p|,|q|)$；而且若 $\alpha\in Z$，则 $h(\alpha)=\log|\alpha|$.

设 K 存在 s 个实嵌入和 2·t 对复嵌入(此时 $D=s+2\cdot t$).根据 Dirichlet 单位定理可知：存在一组 $r=s+t-1$ 个独立的单位 $\varepsilon_1,\cdots,\varepsilon_1$，可使 K 的单位群由

$$\{\zeta\cdot\varepsilon_1^{a_1}\cdots\cdots\varepsilon_r^{a_r}\mid\zeta\text{ 是单位根}, a_i\in Z,\quad i=1,\cdots,r\}$$

给出.K 中仅有有限多个单位根.任何一个可生成单位群无扭部分的独立单位组称为 K 的基本单位组.

若 $a_0=1$,则 α 称为代数整数.元素 $\alpha\in K$ 的范数定义为

$$N_{K/Q}(Q)=\prod_{\sigma}\sigma(\alpha)=[\prod_{i=1}^{d}\alpha_i]^{D/d}$$

对于代数整数 α, $N_{K/Q}(\alpha)\in Z$.K 中的单位恰好是范数 ± 1 的元素.对 K 中两元素 α,β,若存在一个单位 ε,使得 $\alpha=\varepsilon\cdot\beta$,则称 α 与 β 是结合的.设(α)表示由 α 生成的理想,结合的元素生成相同的理想,且同一理想的相异生成元必是结合的.K 中仅存在有限多个非结合的代数整数满足给定范数.设 O_K 表示 K 的代数整数环,如果 O_K 的元素 $\alpha_1,\cdots,\alpha_D$ 是 Q 一线性无关的,则 $Z\cdot\alpha_1\times\cdots\times Z\cdot\alpha_D$ 称为 K 的阶,它是“极大阶”O_K 的子环.

K 中任意代数整数可写成既约元素的积.这里既约元素(素元素)是指除与其自身结合的代数整数以外没有其它整因子的元素.但是,这种分解不必是唯一的.理想也能分解成素理想的乘积,而且这种分解是唯一的.主理想是由单一元素 α 生成的理想.两个分式理想称为等价,若他们的商是主理想.众所周知,仅有有限多个等阶类,它们的个数称为类数 h_K.对于一个理想 a, a^{h_K}必为主理想.整理想 a 的范数定义为

$$N_{K/Q}(a) = \#(o_K/a).$$

对于一个素理想$\mathfrak{p}$,存在一个有理素数 p,使得$\mathfrak{p}$是(p)的一个因子.此时,我们称$\mathfrak{p}$落在 p 上.$\mathfrak{p}$整除(p)的最大次数称为$\mathfrak{p}$的分歧指数,记作$e_{\mathfrak{p}}$,$\mathfrak{p}$的剩余类次数$f_{\mathfrak{p}}$是适合

$$N_{K/Q}(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$$

的整数.素理想$\mathfrak{p}$整除理想 a 的精确幂次数用$\text{ord}_{\mathfrak{p}}(a)$表示.对分式理想 a,这个幂可以是负的.对于数 α,我们将$\text{ord}_{\mathfrak{p}}((\alpha))$写成$\text{ord}_{\mathfrak{p}}(\alpha)$.注意到对所有$\alpha \in K$,可以定义

$$\text{ord}_p(\alpha) = \text{ord}_{\mathfrak{p}}(\alpha)/e_{\mathfrak{p}}.$$

关于这方面的详细内容将在 2·3 节讨论.

2·2 预备引理

本节给出几个简单的备用引理.第一个引理使我们能够对被 logx 的多项式界定的某个实数 $x>1$ 找到一个闭型上界.

引理 2·1 设 $a\geqslant 0$, $h\geqslant 1$, $b>0$, 又设 $x\in R$, $x>1$ 满足

$$x\leqslant a + b\cdot(\log x)^h$$

若 $b>(e^2/h)^h$, 则

$$x<2^h\cdot[a^{1/h} + b^{1/h}\cdot\log(h^h\cdot b)]^h;$$

又若 $b\leqslant(e^2/h)^h$, 则

$$x \leqslant 2^h \cdot [a^{1/h} + 2 \cdot e^2]^h.$$

证明 我们可假定 x 是

$$x = a + b \cdot (\log x)^h$$

的最大解. 由 $(z_1 + z_2)^{1/h} \leqslant z_1^{1/h} + z_2^{1/h}$, 我们导出

$$x^{1/h} \leqslant a^{1/h} + c \cdot \log(x^{1/h}),$$

其中 $c = h \cdot b^{1/h}$, 由 $x^{1/h} = (1 + y) \cdot c \cdot \log c$ 定义 y. 由

$$\log c < \log(c \cdot \log c)$$

导出,

$$c^h \cdot (\log c)^h < b \cdot [\log[c^h \cdot (\log c)^h]]^h,$$

这蕴涵 $x > c^h \cdot (\log c)^h$. 因此 $y > 0$. 现在,

$$\begin{aligned}(1 + y) \cdot c \cdot \log c = x^{1/h} &\leqslant a^{1/h} + c \cdot \log(1 + y) + c \cdot \log c + c \cdot \log\log c \\ &< a^{1/h} + c \cdot y + c \cdot \log c + c \cdot \log\log c\end{aligned}$$

因此

$$y \cdot c \cdot (\log c - 1) < a^{1/h} + c \cdot \log\log c.$$

若 $c \geqslant e^2$, 则导出

$$\begin{aligned}x^{1/h} = c \cdot \log c + y \cdot c \cdot \log c &< c \cdot \log c + \frac{\log c}{\log c - 1} \cdot (a^{1/h} + c \cdot \log\log c) \\ &< 2 \cdot (a^{1/h} + c \cdot \log c)\end{aligned}$$

若 $c \leqslant e^2$，则注意到 $x \leqslant a+(e^2/h)^h \cdot (\log x)^h$，因此，在此情形下可假定 $c=e^2$. 证毕.

以下两个引理说明，无论是实的还是复的 x，若 $|x|$ 很小，则 x 与 $\log(1+x)$ 十分接近.

引理 2·2　设 $a \in R$，若 $a<1$ 且 $|x|<a$，则

$$|\log(1+x)| < \frac{-\log(1-a)}{a} \cdot |x|$$

且

$$|x| < \frac{a}{1-e^{-a}} \cdot |e^x - 1|.$$

证明　注意对 $|x|<1$，$\log(1+x)/x$ 是严格正的和严格减小的函数. 因此对 $|x|<a$，它总是比它取 $x=-a$ 时得到的值小. 对函数 $x/(e^x-1)$ 也有同样的结论.

引理 2·3　设 $0<a\leqslant\pi$，若 $|x|<a$，则

$$|x| < \frac{a}{2 \cdot \sin(a/2)} \cdot |e^{i \cdot x} - 1|$$

若 $a<2$，$|e^{i\cdot x}-1|<a$ 且 $|x|<\pi$，则

$$|x| < \frac{2 \cdot \arcsin(a/2)}{a} \cdot |e^{i \cdot x} - 1|.$$

证明　注意到 $|e^{i\cdot x}-1| = 2 \cdot |\sin(\frac{1}{2} \cdot x)|$，又 $2 \cdot \sin(\frac{1}{2} \cdot x)/x$ 是正偶函数，在 $0 \leqslant x < a$ 上减小，因此它在 $x=a$ 处取得最小值. 第一个不等式已导出. 第二个不等式可用类似方法证得.

2·3 p－adic 数及其函数

本节给出以后将要用到的关于 p－adic 数及其函数的结果，详细证明可参考文献[6]，[57]，[58].

我们假定读者熟知 p－adic 数域 Q_p 及 p－adic 赋值 ord_p. 注意到 ord_p 寻常定义在 Q_p 上，与 2·1 节给出的定义相一致. 我们用 Ω_p 表示 Q 的代数闭包的整体，即对此域所有 P－adic 理论都能应用.

每一个非零数 $\alpha \in Q_p$ 有 p－adic 展式

$$\alpha = \sum_{i=k}^{\infty} u_i \cdot p^i,$$

其中 $k = ord_p(\alpha)$，p－adic 数字 u_i 在(0, 1, …, p－1)中取值，满足 $u_k \neq 0$. 在此情形下，数 0 可通过取 k＝0 及所有数字等于 0 来表示，并定义 $ord_p(0) = \infty$. 若 $ord_p(\alpha) \geqslant 0$，则 α 称为 p－adic 整数. p－adic 整数集用 Z_p 表示. 一个 p－adic 单位是 $\alpha \in Q$ 满足 $ord_p(\alpha) = 0$. 对于任意 p－adic 整数 α 及任意 $\mu \in N_0$，存在唯一有理整数 $\alpha^{(\mu)} = \sum_{i=0}^{\mu-1} u_i p^i$ 满足

$$ord_p(\alpha - \alpha^{(\mu)}) \geqslant \mu, \quad 0 \leqslant \alpha^{(\mu)} \leqslant p^{\mu} - 1.$$

对于 $ord_p(\alpha) \geqslant k$，我们也写成 $\alpha \equiv 0 (mod p^k)$. p－adic 范数定义为

$$|\alpha|_p = P^{-ord_p(\alpha)}.$$

在 2·1 节我们已看到如何在 Q 的代数扩张上定义 ord_p

及 ord_p. 对任意满足 $\mathrm{ord}_p(\alpha)>1/(P-1)^p$ 的 $\alpha\in\Omega_p$, 我们可以定义 p-adic 对数 $\log_p(1+\alpha)$ 为泰勒级数

$$\log_p(1+\alpha)=\alpha-\alpha^2/2+\alpha^3/3-\cdots$$

这个对数函数有熟知的对数性质. 有如 $\log_p(\xi_1\cdot\xi_2)=\log_p(\xi_1)+\log_p(\xi_2)$ 对已定义的所有 ξ_1,ξ_2 成立. 进而, $\log_p(\xi)=0$ 当且仅当 ξ 是一个单位根时成立. 在 Q_p 中仅有的单位根是第 $(p-1)$ 个单位根(若 p 是奇数). 运用这些性质, 这个对数函数扩充到所有满足 $\mathrm{ord}_p(\xi)=0$ 的 $\xi\in\Omega_p$. 由费马定理, 对于代数数域存在 $k\in N$ 使得 $\mathrm{ord}_p(\xi^k-1)>1/(p-1)$, 则

$$\log_p(\xi)=\frac{1}{k}\cdot\log_p[1+(\xi^k-1)].$$

一个等价定义是 $\log_p(\xi)=\log_p(\xi/\zeta)$, 其中 ζ 是单位根, 使得 $\mathrm{ord}_p(\xi-\zeta)>0$. 用这种方式, p-adic 对数是恰当定义的函数. 注意 $\log_p(\xi)$ 落在由 ξ 生成的 Ω_p 的子域内. 最后, 我们注意到, 如若 $\mathrm{ord}_p(\xi)>1/(p-1)$, 则

$$\mathrm{ord}_p(\xi)=\mathrm{ord}_p(\log_p(1+\xi)).$$

2·4 对数线性型的下界

本节我们引入要用到的 Gelfond - Baker 理论的详细结果. 他们导出代数数的对数线性型的下界. 我们通常不给出这些定理的充分一般的情形, 因为本书仅出现未知有理数的线性型, 尽管 Gelfond - Baker 定理几乎都是对未知代数数的线性型提出的. 我们选择完全显示的常数界, 因为仅有这种彻底

显示的结果能为我们的宗旨所使用.

具有至少三项的对数线性型方面的第一个结果应归于 Baker[7],而在 p-adic 情形应归于 Coates. 关于这一理论的综述可参考文献[10]、[132]. 我们将应用更新近、更强的结果,归于 Baker 和 Wüstholz[12]、[133]和于坤瑞[142],[143].

首先论及实的或复的对数线性型. 我们引进 Baker 和 Wüstholz[12]以及 Waldschmidt[133]的结果:

引理 2·4　设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是非零代数数, $K=Q(\alpha_1,\alpha_2,\cdots,\alpha_n)$的次数等于 D. 如果对于整数 $b_1,b_2,\cdots,b_n$, $\Lambda=b_1\log\alpha_1+b_2\log\alpha_2+\cdots+b_n\log\alpha_n\neq 0$, 则必有

$$|\Lambda|\geqslant\exp(-C(n)D^{n+2}(\log n+\log D)(\prod_{i=1}^{n}\log A_i)(\log B)),$$

其中

$$C(n,D)<\min(2^{5n+10}.18(n+1)!\ \ n^{n+1},2^{6n+32}n^{3n+6}),$$

$$\log A_i=\max(\frac{1}{D},\frac{|\log\alpha_i|}{D},h(\alpha_i)),\quad i=1,2,\cdots,n,$$

$$B=\max(2,|b_1|,|b_2|,\cdots,|b_n|).$$

有关引理 2·4 中常数的改进情况还可参考 Blass, Glass, Manski, Meronk 和 Steiner[19],[20], Loxton, Mignotte, Van der Poorten 和 Waldschmidt[70], Philippon 和 Waldschmidt[94],以及 Wüstholz[140]等人的工作. 对于 n=2 的情形,明

显的上界已由 Mignotte 和 Waldschmidt[81],[82]给出. 再改进由 Laurent、Mignotte 和 Nesterenko[62]给出.

在 p - adic 情形, 我们引进两个结果: 一个归于 Schinzel [101](定理 1), 是关于具有两项的对数线性型的情形, 另一个关于一般情形的应归于于坤瑞[141](也可参阅于坤瑞[142]). 我们注意到于坤瑞的界大大改进了上面 Van der Poorten[98]的结果, 而且还改正了文献[98]中的一些错误.

引理 2·5(Schinzel)　设 P 是素数, 设 Δ 是无平方整数, 设 D 是 $K = Q(\sqrt{\Delta})$ 的判别式. 设 $\xi = \xi''/\xi'$ 及 $x = x''/x'$ 是 K 的元素, 其中 ξ', ξ'', x', x'' 是代数整数. 令

$$L = \log\max[|e \cdot D|^{1/4}, \|\xi' \cdot x'\|, \|\xi' \cdot x''\|, \|\xi'' \cdot x'\|, \|\xi'' \cdot x''\|],$$

这儿 $\|r\|$ 表示 $r \in K$ 的共轭的最大绝对值. 设 $\mathfrak{p}$ 是 K 的素理想, 满足范数 $N_{\mathfrak{p}} = P^{\rho}$. 设 $\psi = 2/p \cdot \log P$, $\varphi = \mathrm{ord}_{\mathfrak{p}}(p)$. 若 ξ 或 x 是一个 p - adic 单位而且 $\xi^n \neq x^n$, 则

$$\mathrm{ord}_{\mathfrak{p}}(\xi^n - x^m) < 10^6 \cdot \psi^7 \cdot \varphi^{-2} \cdot L^4 \cdot p^{4\rho+4} \cdot [\log\max(|m|, |n|) + \varphi \cdot L \cdot p^{\rho} + 2/L]^3$$

引理 2·6(于坤瑞)　设 $\alpha_1, \cdots, \alpha_n (n \geqslant 2)$ 是非零代数数. 令 $L = Q(\alpha_1, \cdots, \alpha_n)$, $d = [L:Q]$. 设 $b_1, \cdots, b_n$ 是有理整数. 设 $\mathfrak{p}$ 是 L 的一个素理想, 落在有理素数 p 上. 设 $e_{\mathfrak{p}}$ 是分歧指数, $f_{\mathfrak{p}}$ 是 $\mathfrak{p}$ 的同余类次数. L 关于 $\mathrm{ord}_{\mathfrak{p}}$ 的整体写成 $L_{\mathfrak{p}}$(则对所有 $\beta \in L_{\mathfrak{p}}$, 我们有 $\mathrm{ord}_{\mathfrak{p}}(\beta) = e_{\mathfrak{p}} \cdot \mathrm{ord}_{p}(\beta)$. 设 q 是一个有理素数使得

$$q \nmid p \cdot (p^{f_{\mathfrak{p}}} - 1).$$

又设

$$V_j \geqslant \max[h(\alpha_j), f_\wp \cdot (\log p)/d], j=1, \cdots, n.$$

使得

$$V_1 \leqslant \cdots \leqslant V_{n-1}, \quad V_{n-1}^+ = \max(1, V_{n-1}).$$

$$B_0 \geqslant \min_{1\leqslant j\leqslant n, b_j\neq 0} |b_j|, \quad B_n \geqslant |b_n|, \quad B' \geqslant \max_{1\leqslant j\leqslant n-1} |b_j|$$

$$B \geqslant \max[|b_1|, \cdots, |b_n|, 2],$$

$$W \geqslant \max[\log(1+\frac{3}{4\cdot n}\cdot B, \log B_0, f_\wp \cdot (\log p)/d].$$

假定对 $j=1, \cdots, n, \mathrm{ord}_\wp(\alpha_j)=0$, 则

$$[L(\alpha_1^{1/q}, \cdots, \alpha_n^{1/q}) : L = q_n \tag{2·1}$$

则 $\mathrm{ord}_p(b_n) \leqslant \mathrm{ord}_p(b_j), j=1, \cdots, n$, 且 $\alpha_1^{b_1}\cdots, \alpha_n^{b_n} \neq 1$. 那么

$$\mathrm{ord}_\wp[\alpha_1^{b_1}\cdots\alpha_n^{b_n}-1] < c_1(p,n)\cdot a_1^n \cdot n^{n+5/2}\cdot q^{2\cdot n}\cdot(q-1)\cdot$$

$$\cdot \log^2(n\cdot g)\cdot(p^{f_\wp}-1)\cdot(2+\frac{1}{p-1})^n\cdot(f_\wp\cdot(\log p)/d)^{-(n+2)}.$$

$$\cdot V_1\cdots V_n\cdot[\frac{W}{6\cdot n}+\log(4\cdot d)]\cdot[\log(4\cdot d\cdot V_{n-1}^+ +$$

$$\cdot f_\wp\cdot(\log p)/8\cdot n],$$

其中　当 $n\leqslant 7$ 时, $a_1 = 56\cdot e/15$;

　　　当 $n\geqslant 8$ 时, $a_1 = 8\cdot e/3$.

而 $c_1(p,n)$ 由下表给出，对 $p \geq 5$，

$$c_1(p,n) = c'_1(p,n) \cdot \left(2 + \frac{1}{p-1}\right)^2$$

n	2	3	4	5	6	7	≥8
$c_1(2,n)$	768523	476217	373024	318871	284931	261379	2770008
$c_1(3,n)$	167881	104028	81486	69657	62243	57098	116055
$c'_1(p,n)$	87055	53944	42255	36121	32276	24584	311077

注　于坤瑞[143]给出的结果中，删除了"独立条件"(2·1)，具有更多或更少的相同常数.这一结果当 $d \geq 1$ 时更易于应用.

2·5　数值方法

根据丢番图逼近理论，用计算的方法解丢番图方程，正如我们将在第 4 至第 8 章所进行的，有必要取代数数对数(实的、复的或 p－adic 的)有效的足够大的精度(可以是数百个数位).我们将不深入到计算这样的逼近问题，而只在本节给出几点注记.

首先，多数计算机(主机以及专用机)计算的精度不满足我们的要求.通常至多是达到二倍精度(52 位二进位数，等价于 15 位十进位数字)，或者至好也不过四倍精度(112 位二进位数，等价于 33 位十进位数).这不能充分满足我们的要求，不仅因为我们要求更高的精度，也因为我们想把舍入误差控

制住，使丢番图方程确实没有解被舍入误差的意外影响而遗漏.

具有任意精度的计算程序包是可得到而且很有用的. 例如，R. P. Brent 的 MP 程序包(参见文献[24]). 同样地，我们为简单的多精度数计算编写自己的程序包是不难的，例如加法、乘法和除法(为有效计算，参阅文献[56]). 据作者所知，目前还没有公开的 p－adic 数方面的计算程序可以得到. 但对实数，其程序相类似，因此相对地容易(虽然可能是麻烦的)自己编出.

计算整系数多项式的根可用牛顿方法，在实的及 p－adic 的情形. 获得的结果必须正确也就是要求的精度正确，不仅找到的近似根代入多项式并验证其结果在要求的精度内是 0，而且对牛顿方法也要进行理论误差估计，或用“区间运算”(见下面).

计算对数也可用牛顿方法，但我们发现用泰勒级数

$$\log(1+x)=x-x^2/2+x^3/3-\cdots$$

更容易. 或用收敛更快的级数

$$\log\frac{1+x}{1-x}=2[x+x^3/3+x^5/5+\cdots],$$

当 $|x|$ 很小时，这种方法快，而对较大的 $|x|$，下面的方法好. 比如计算逼近于所需精度的 log1. 1，log1. 0001，log1. 00000001，将其保留. 现在计算 $x_1\in[1,1.1]$ 和 $k_1\in N_0$，使得

$$x=x_1\cdot 1.1^{k_1}$$

这仅是小分子和分母(11 和 10)的有理数的多精度数除法的

一些问题，能做得快. 其次计算 $x_2 \in [1, 1.00000001]$ 和 $k_3 \in N_0$，使得

$$x_2 = x_3 \cdot 1.00000001^{k_3}.$$

然后用泰勒级数计算 $\log x_3$，其收敛非常快，并由

$$\log x = \log x_3 + k_3 \cdot \log 1.00000001 + k_2 \cdot \log 1.0001 + k_1 \cdot \log 1.1$$

计算 $\log x$. 所有这些计算，都必须留心控制住每一个加法或乘法出现偏离的错误. 以运用"区间运算"的做法为例，即对所有运算，两次取比实际需要略多的数字，每一步偏离不同的方向. 然后，得到充分小区间，精确数就落在该区间内(具有数学的必然).

arctanx 通过泰勒级数

$$\operatorname{arctg} x = x - x^3/3 + x^5/5 - \cdots$$

计算. 数 $\pi = 3.14159\cdots$ 可通过恒等式

$$\pi = 16 \cdot \arctan 1/5 - 4 \cdot \arctan \frac{1}{239}$$

用此泰勒级数对反正切函数来迅速计算.

进行 p - adic 运算优于上面实运算，偏离不会趋于更大，只要不被具有正 p - adic 次数的数整除. 若 $\operatorname{ord}_p(x) > 0$，则 $\log_p(1+x)$ 可通过泰勒级数

$$\log_p(1+x) = x - x^2/2 + x^3/3 \cdots$$

计算，也可用

$$\log_p \frac{1+x}{1-x} = 2[x + x^3/3 + x^5/5 + \cdots]$$

计算.若 $x \neq 0 \pmod p$ 且 $x \neq 1 \pmod p$,则 $\log_p x$ 可计算,因为存在一个 $k \in N$ 使得 $x^k \equiv 1 \pmod p$,则

$$\log_p x = \frac{1}{k} \log_p [1 + (x^k - 1)].$$

而上面给出的泰勒级数可用于计算 $\log_p x$.注意在计算上述泰勒级数时,各项的分母中有因子 p.因此,找出 $\log_p(1+x)$ 的前 μ 个 p-adic 数字,仅计算泰勒级数前面 $\mu/\text{ord}_p(x)$ 项是不够的,但前 k 项必须重视,其中 k 是满足

$$k \cdot \text{ord}_p(x) - \log k / \log p \geqslant \mu$$

的最小整数.

为了泰勒级数快速收敛,仅对具有大 p-adic 次数的数 x 应用泰勒级数是合符需要的.例如

$$\log_3 4 = 3 - 3^2/2 + 3^3/3 - \cdots$$

收敛速度不如

$$\log_3 4 = \frac{1}{3} \log_3 64 = \frac{1}{3} [7 \cdot 3^2 - 7^2 \cdot 3^4/2 + 7^3 \cdot 3^6/3 - \cdots]$$

快,或不如

$$\log_3 4 = \log_3 \frac{1 + 3/5}{1 - 3/5} = 2[3/5 + 3^3/3 \cdot 5^3 + 3^5/3 \cdot 5^5 + \cdots]$$

快,或不如

$$\log_3 4 = \frac{1}{3}\log_3 \frac{1+7\cdot 3^2/65}{1-7\cdot 3^2/65}$$

$$= \frac{2}{3}[7\cdot 3^2/65 + 7^3\cdot 3^6/3\cdot 65^3 + 7^5\cdot 3^{10}/5\cdot 65^5 + \cdots]$$

快.

如 3·5 节所述，对于 L^3－运算的有效、确切的完成，上述考虑是充分的．我们对某些常数也运用简单连分数计算．做法如下．假定我们要计算一个实数 v 的连分数展式，可用有理数 v_1, v_2 来逼近，使得对某个小 ε，

$$v_1 < v < v_2 < v_1 + \varepsilon$$

我们可精确计算 v_1, v_2 的连分数展式，直至他们恰好相合，便是 v 的连分数展式．若对给定（大的）常数 X_0，v 的连分数展式需要到分母 $q_k > X_0$ 的第 k 项收敛，则 ε 最小必须小到 X_0^{-2}.

第三章　丢番图逼近的计算

3·1　导言

本节叙述用于降低丢番图方程解的上界的计算方法. 我们的出发点总是接近于 0 的线性型 Λ(在实的或 p－adic 的意义下. 其中“接近”明确定义为包含未知数的一个不等式), 此线性型具有关于 Λ 的系数的绝对值的大的但确切知道的上界. 我们的目的是通过证明在新的上界和原来的上界之间没有解而降低上界.

设 $v_1, \cdots, v_n, \beta$ 给定, 属于 R 或属于关于固定素数 P 的 Ω_p. 设 $x_1, \cdots, x_n$ 是 Z 中的未知数. 令

$$\Lambda = \beta + \sum_{i=1}^{n} x_i \cdot v_i .$$

我们按以下三条标准把这一线性型分类:

→齐次的, 若 $\beta=0$, 非齐次的, 若 $\beta\neq 0$;

→一维的, 若 $n=2$, 多维的, 若 $n\geqslant 3$;

→实的, 若对所有 i, $v_i\in R$, p－adic 的, 若对所有 i, $v_i\in \Omega_p$.

$n=2$ 时称其为一维的理由是在线性型

$$\Lambda = x_1 \cdot v_1 + x_2 \cdot v_2$$

的齐次情形下, 归为研究一维连分数的 $-v_1/v_2$ 的展式的简单

情形.满足 $n=1$ 的非齐次情形,就是说

$$\Lambda=\beta+x\cdot v$$

在实的情形我们没有任何兴趣,但在 p - adic 的情形我们是感兴趣的.我们将这种情形称为零维的.

在 p - adic 情形我们要求分数 v_i/v_j 和 β/v_j 属于 Q_p 本身,而数 v_i,β 容许是某较大的 Ω_p 的子域中的数.

设 c,δ 是正常数,令 $X=\mathrm{mac}|x_i|$,设 X_0 是一个(大)正常数.在实的情形,我们总假定

$$|\Lambda|<c\cdot\exp(-\delta\cdot X) \tag{3·1}$$

$$X\leqslant X_0 \tag{3·2}$$

设 c_1,c_2 是满足 $c_2>0$ 的实常数.在 p - adic 情形我们将假定 $x_j>0$,对某些下标 $j\in(1,\cdots,n)$,且

$$\mathrm{ord}_p(\Lambda)\geqslant c_1+c_2\cdot x_j \tag{3·3}$$

$$X\leqslant X_0 \tag{3·4}$$

我们的目的是找到一个与 $\log X_0$ 一样大小的常数 X_1,使得在实的情形(3·2)能替换成 $X\leqslant X_1$,在 p - adic 情形,界 $x_j\leqslant X_0$((3·4)的推论)能改进为 $x_j\leqslant X_1$.

在以后的各节中,我们将按照上面给出的分类讨论所有情形.我们在 L^3 - 运算方面插入 3·4,3·5 节,这是我们主要的计算工具.3·6 节找出格中的短向量,3·13 是足够我们用的关于某些子格方面的.

3·2 实的情形的齐次一维逼近:连分数

我们首先研究

$$\Lambda = x_1 \cdot v_1 + x_2 \cdot v_2$$

的情形. 令 $v = -v_1/v_2$, 我们假定 v 是无理数. 设 v 的连分数表达式由

$$v = [a_0, a_1, a_2, \cdots]$$

给出. 并设对 $n = 0, 1, 2, \cdots$, 渐近分数 p_n/q_n 由

$$\begin{cases} p_{-1} = 1, p_0 = a_0, p_{n+1} = a_{n+1} p_n + p_{n-1} \\ q_{-1} = 0, q_0 = 1, q_{n+1} = a_{n+1} q_n + q_{n-1} \end{cases}$$

定义. 众所周知, 此渐近分数满足不等式

$$\frac{1}{(a_{n+1}+2) \cdot q_n^2} < \left| v - \frac{p_n}{q_n} \right| < \frac{1}{a_{n+1} \cdot q_n^2} \tag{3·5}$$

且当 p/q 满足不等式

$$\left| v_2 - \frac{p}{q} \right| < \frac{1}{2 \cdot q^2} \tag{3·6}$$

时, p/q 必为渐近分数(参考 Hardy 和 Wright[53], 定理 163, 171, 184).

不失一般性, 我们假定 $|v_1| < |v_2|$, $x_1 > 0$, $(x_1, x_2) = 1$. 由(3·1)导出, 存在一个数 X^*, 使得 $X \geq X^*$, 蕴涵 $X = x_1$ 以及(3·6)式中 $(p, q) = (-x_2, x_1)$. 现在, 我们有下面准则.

引理 3·1　(i)若(3·1)和(3·2)对于满足 $X \geqslant X^*$ 的 x_1, x_2 成立，则 $(-x_2, x_1) = (p_k, q_k)$ 对于下标 k 满足

$$k \leqslant -1 + \log[\sqrt{5} \cdot X_0 + 1] / \log[\frac{1}{2}(1+\sqrt{5})] \tag{3·7}$$

进而，部分分式 a_{k+1} 满足

$$a_{k+1} > -2 + |v_2| \cdot c^{-1} \cdot \exp(\delta \cdot q_k) / q_k \tag{3·8}$$

(ii) 若对某个 k 满足 $q_k \geqslant X^*$

$$a_{k+1} > |v_2| \cdot c^{-1} \cdot \exp(\delta \cdot q_k) / q_k \tag{3·9}$$

则(3·1)对于 $(-x_2, x_1) = (p_k, q_k)$ 成立.

证　(i) 对下标 k，由 $X \geqslant X^*$ 和(3·6)得到 $(-x_2, x_1) = (p_k, q_k)$. 因为 q_k 最小是第(k+1)个 Fibonacci，由 $q_k = x_1 = X = X_0$ 导出(3·7). 为证(3·8)，只需应用(3·1)用(3·5)的第一个不等式.

(ii) 结合(3·5)第二个不等式及(3·9)即得

我们也可直接应用引理 3.1(i)如下：

引理 3·2　设

$$A = \max(a_{k+1})$$

其中最大值是取遍满足(3·7)的所有下标 k，若(3·1)和(3·2)对于满足 $X \geqslant X_1$ 的 x_1, x_2 成立，则

$$X < \frac{1}{\delta} \cdot \log[c \cdot (A+2) / |v_2|] + \frac{1}{\delta} \cdot \log X$$

注：从引理 3·2 导出 X 的一个上界. 这里我们可应用引理 2·1，但引理 2·1 显然仅对大的 b 成立.

证 (3·1)和(3·5)导出

$$(a_{n+1}+2)\cdot q_n^2 > q_n\cdot|v_2|/|\Lambda| > q_n\cdot|v_2|\cdot c^{-1}\cdot\exp(\delta\cdot X).$$

引用引理(3·1)(i)便导出结论.

实际上,Λ 很大的情况并非经常出现,因此这个引理能充分满足需要.

概而言之,这种情况产生计算一个实数的连分数直到一定精确度,并且证实没有极端大的部分商.这一想法已被 Ellison[37], Cijsouw, Karllaar 和 Tijdeman(参见 Stroeker 和 Tijdeman[114]的附录)等人应用于实际,同时,被 Steiner[109]应用于关于 Syracuse(“3·N+1”)问题,被 Cherubini 和 Wallisser[31](仅用微型计算机)用于确定所有具有类数 1 的虚二次域.我们将在第 4、第 5 章中介绍这方面的结果.

3·3 实情形的非齐次一维逼近:Davenport 引理

以下情形只对 Λ 具有以下形式时论述:

$$\Lambda=\beta+x_1\cdot v_1+x_2\cdot v_2,$$

其中 $\beta\neq0$.这样我们可以应用 Baker 和 Davenport[11]引入的所谓 Davenport 引理.这正如齐次的情形,是基于连分数计算.

设 $v=-v_1/v_2$, $\psi=\beta/v_2$,则有

$$\frac{\Lambda}{v_2}=\psi-x_1\cdot v+x_2.$$

设 p/q 是 v 的满足 $q>X_0$ 的渐近分数.我们有下面结果.

引理 3·3(Davenport)记号如上述，假定

$$\| q\cdot\psi \| > 2\cdot X_0/q \qquad (3\cdot 10)$$

(用 $\|\cdot\|$ 表示到最近整数的距离). 则(3·1)和(3·2)的解满足

$$X < \frac{1}{\delta}\cdot\log[q^2\cdot c/|v_2|\cdot X_0] \qquad (3\cdot 11)$$

证　由(3·5)和(3·10)推出

$$\begin{aligned} 2\cdot X_0/q &< \| q\cdot(\psi - x_1\cdot v + x_2) + x_1\cdot(q\cdot v - p) \| \\ &< q\cdot|\Lambda/v_2| + |x_1|/q. \end{aligned}$$

由(3·1),(3·2)以及

$$X_0 < q^2\cdot c\cdot|v_2^{-1}|\cdot\exp(-\delta\cdot X)$$

便导出(3·11).

若(3·10)确实不是满足分母大于 X_0 的渐近分数，则必须尝试某一个进一步的渐近分数. 若 q 实质上不比 X_0 大，则(3·11)导出正合要求的 X 的降低了的上界，其大小为 $\log X_0$. 若满足(3·10)大小为 X_0 的 q 找不到(经验表明，这种情形极不可能发生)，则并不失去解，因为仅有少许例外的可能解必须验证. 详见 Baker 和 Davenport[11].

概而言之，我们看到，这种情形的基本思想是：(3·1)和(3·2)的非常大的解导出 v 的渐近分数 p/q 的大范围，其中 $\| q\cdot\psi\|$ 的值都非常小. 实际上出现的情形，$q\cdot\psi$ 总是离最接近的整数足够远($\| q\cdot\psi\|$ 几乎是随机分布在区间[0,0.5]上). 这一方法的实际运用者有我们已经说过的 Baker 和 Davenport

[11], 还有 Ellison, Pesek, Stahl 和 Stall[38], Steiner[110], Gaal[44]. 我们将在第 4 章应用. 注意到我们在 3·8 节对多维的非齐次情形的讨论方法, 正好也能应用于一维的情形. 这已被 de Weger[138]所论证.

3·4 L^3 – 格基简化运算, 理论

为了论及具有 $n \geqslant 3$ 的线性型, $n = 2$ 的情况的简单推广, 必须研究多维连分数. 这方面好的通论参看 Brentjes[25]. 然而, 这方面的有效计算似乎没有令人满意的效率和一般原则. 幸亏自从 1981 年有了一定意义上也是一般化的一维连分数计算的实用选择.

在 1981 年, L. Lovásg 创造一种计算, 后来成了熟知的 L^3 – 运算. (见 Lenstra, Lenstra 和 Lovász[69], 图表 1, 521 页). 从一个 R^n 中的格的任意基到这个格的另一个所谓简化基的运算, 有着某些优美的性质(其向量接近于正交).

此运算在各个数学领域有许多重要应用, 有如多项式的因式分解(见 Lenstra[68]), 公共键密码学(参见 Lagarias and Odlyzko[60]), 反证 Mertens 猜想(参见 Odlyzko and te Riele[87]). 我们感兴趣的是它在丢番图逼近方面的应用, 这已在文献[69], 525 页中指出. 此运算有着很好的理论上的复杂性, 而且对实际计算的完成也非常好.

设 $\Gamma \subset R^n$ 是一个格, 它由基 $\underline{b}_1, \cdots, \underline{b}_n$ 给出. 我们按照文献[69]516 页, 导入 Γ 的简化基的概念. 向量 $\underline{b}_i^*$ $(i = 1, \cdots, n)$ 和实数 μ_{ij} $(1 \leqslant j < i \leqslant n)$ 归纳地定义为

$$\underline{b}_i^* = \underline{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \cdot \underline{b}_j^*, \quad \mu_{i,j} = (\underline{b}_i, \underline{b}_j^*)/(\underline{b}_j^*, \underline{b}_j^*).$$

则 $\underline{b}_1^*, \cdots, \underline{b}_n^*$ 是 R_n 的一个正交基.我们称 Γ 的格基 $b_{\underline{1}}, \cdots, b_{\underline{n}}$ 为简化基,若

$$|\mu_{i,j}| \leqslant \frac{1}{2}, \quad 1 \leqslant j < i \leqslant n$$

$$|\underline{b}_i^* + \mu_{i,i-1} \cdot \underline{b}_{i-1}^*|^2 \geqslant \frac{3}{4} \cdot |\underline{b}_{i-1}^*|^2, \quad 1 < i \leqslant n.$$

因此一个简化基是近似于正交的.对于一个简化基 $b_{\underline{1}}, \cdots, b_n$,文献[69]中(1·7),有

$$|\underline{b}_i^*| \geqslant 2^{-(n-1)/2} \cdot |\underline{b}_1|, \quad i = 1, 2, \cdots, n \qquad (3 \cdot 12)$$

我们注意到,一个格可以有多于一个的简化基,其基向量的顺序关系不是任意的.L^3-运算就是输入 Γ 的任意基 $\underline{b}_1, \cdots, \underline{b}_n$,并计算出该格的一个简化基 $\underline{c}_1, \cdots, \underline{c}_n$.我们往往感兴趣的简化基的性质如下.设 $\underline{y} \in R^n$ 是给定点,它不是格点.我们用 $l(\Gamma)$表示该格中最短的非零向量的长,就是说

$$l(\Gamma) = \min_{0 \neq x \in \Gamma} |\underline{x}|.$$

用 $l(\Gamma, \underline{y})$表示从 $\underline{y}$ 到最近的格点的距离,即

$$l(\Gamma, \underline{y}) = \min_{\underline{x} \in \Gamma} |\underline{x} - \underline{y}|$$

根据下面的结果,由简化基,$l(\Gamma)$和 $l(\Gamma, \underline{y})$的下界能计算出来.引理 3·4 是文献[69]中的命题(1·11).我们这里重视其证明,以显示引理 3·4 和 3·5 的证明是相似的.

引理 3·4(Lenstra, Lenstra 和 Lovasz[69]) 设 $\underline{c}_1, \cdots, \underline{c}_n$ 是格 Γ 的简化基,则

$$l(\Gamma) \geqslant 2^{-(n-1)/2} \cdot |\underline{c}_1|$$

证 设 $\underline{0} \neq \underline{x} \in \Gamma$ 是具有最小长 $|\underline{x}| = l(\Gamma)$ 的格点. 记

$$\underline{x} = \sum_{i=1}^{n} r_i \cdot \underline{c}_i = \sum_{i=1}^{n} r_i^* \cdot \underline{b}_i^*$$

满足 $r_i \in Z$, $r_i^* \in R$. 设 i_0 是使 $r_{i_0} \neq 0$ 的最大下标,则由于对所有 i, $\underline{c}_1, \cdots, \underline{c}_i$ 与 $\underline{b}_1^*, \cdots, b_i^*$ 生成相同的线性空间,且 $\underline{b}_{i+1}^*$ 是 $\underline{c}_{i+1}$ 在这个线性空间的正交补上的投影,这就导出 $r_{i_0} = r_{i_0}^*$. 因此,由(3·12),有

$$l(\Gamma)^2 = |\underline{x}|^2 = \sum_{i=1}^{i_0} r_i^{*2} \cdot |\underline{b}_i^*|^2 \geqslant r_{i_0}^{*2} \cdot |\underline{b}_{i_0}^*|^2 = r_{i_0}^2 \cdot |\underline{b}_{i_0}^*|^2$$
$$\geqslant |\underline{b}_{i_0}^*|^2 \geqslant 2^{-(n-1)} \cdot |\underline{c}_1|^2.$$

引理 3·5 设 $\underline{c}_1, \cdots, \underline{c}_n$ 是格 Γ 的简化基,又设 $\underline{y} = \sum_{i=1}^{n} s_i \cdot \underline{c}_i$, $s_1, \cdots, s_n \in R$, s_i 不全属于 Z, 设 i_0 是使 $s_{i_0} \notin Z$ 的最大下标,则

$$l(\Gamma, \underline{y}) \geqslant 2^{-(n-1)/2} \cdot \| s_{i_0} \| \cdot |\underline{c}_1|.$$

证 设 $\underline{x} \in \Gamma$ 是最接近 $\underline{y}$ 的格点,因此 $|\underline{x} - \underline{y}| = l(\Gamma, \underline{y})$. 记

$$\underline{x}=\sum_{i=1}^{n} r_i \cdot \underline{c}_i=\sum_{i=1}^{n} r_i^* \cdot \underline{b}_i^*, \quad \underline{y}=\sum_{i=1}^{n} s_i \cdot \underline{c}_i=\sum_{i=1}^{n} s_i^* \cdot \underline{b}_i^*.$$

其中 $r_i \in Z, r_i^*, s_i, s_i^* \in R$. 设 i_1 是使得 $r_{i_1} \neq s_{i_1}$ 得的最大下标，则如同证明引理 3·4 的理由，我们得到

$$r_{i_1}-s_{i_1}=r_{i_1}^*-s_{i_1}^*.$$

由(3·12)导出

$$l(\Gamma, \underline{y})^2 \geqslant (r_{i_1}-s_{i_1})^2 \cdot |\underline{b}_{i_1}^*|^2 \geqslant (r_{i_1}-s_{i_1})^2 \cdot 2^{-(n-1)} \cdot |\underline{c}_1|^2$$

显然，$i_1 \geqslant i_0$，若 $i_1=i_0$，立即得到结论；若 $i_1>i_0$，则 $s_{i_1} \in Z, s_{i_1} \neq r_{i_1}$，因此，$|r_{i_1}-s_{i_1}| \geqslant 1$. 由此证得了结论.

上述引理在 s_{i_0} 非常接近一个整数的特别情况下是相当弱的. 假定另一个 s_i 不接近一个整数，我们可应用下面的变形.

引理 3·6　设 $\underline{c}_1, \cdots, \underline{c}_n$ 是格 Γ 的一个简化基，$\underline{y}=\sum_{i=1}^{n} s_i \cdot \underline{c}_i$，其中 $s_1, \cdots, s_n \in R (i=1, \cdots, n)$，满足 s_i 不全属于 Z. 假定存在一个下标 i_0 和常数 $\delta_1, 0<\delta_2<\frac{1}{2}$，使得

$$\| s_i \| \leqslant \delta_1, \quad i=i_0+1, \cdots, n$$

$$\| s_{i_0} \| \geqslant \delta_2.$$

则

$$l(\Gamma, \underline{y}) \geqslant 2^{-(n-1)/2} \cdot \delta_2 \cdot |\underline{c}_1| - (n - i_0) \cdot \delta_1 \cdot \max_{i>i_0} |\underline{c}_i|$$

证 采用证明引理 3·5 的记号，设 t_i 是最接近 s_i 的整数，其中 $i \geqslant i_0 + 1$，又对 $i \leqslant i_0$，$t_i = s_i$，令

$$\underline{z} = \sum_{i=1}^{n} t_i \cdot \underline{c}_i = \sum_{i=1}^{n} t_i^* \cdot \underline{b}_i^*$$

满足 $t_i^* \in R$. 设 i_1 是满足 $r_{i_1} \neq t_{i_1}$ 的最大下标. 则

$$r_{i_1} - t_{i_1} = r_{i_1}^* - t_{i_1}^*$$

有

$$l(\Gamma, \underline{y}) = |\underline{x} - \underline{y}| \geqslant |\underline{x} - \underline{z}| - |\underline{z} - \underline{y}|$$

现在

$$|\underline{z} - \underline{y}| \leqslant \sum_{i=i_0+1}^{n} |s_i - t_i| \cdot |\underline{c}_i| \leqslant (n - i_0) \cdot \delta_1 \cdot \max_{i>i_0} |\underline{c}_i|$$

应用(3·12)，有

$$\begin{aligned}|\underline{x} - \underline{z}|^2 &= \sum_{i=1}^{n} (r_i^* - t_i^*)^2 \cdot |\underline{b}_i^*|^2 \\ &\geqslant (r_{i_1}^* - t_{i_1}^*)^2 \cdot |\underline{b}_{i_1}^*|^2 \\ &\geqslant (r_{i_1} - t_{i_1})^2 \cdot 2^{-(n-1)} \cdot |\underline{c}_1|^2.\end{aligned}$$

显然，$i_1 \geqslant i_0$. 若 $i_1 = i_0$，即得结论. 若 $i_1 > i_0$，则 $t_{i_1} \in Z$，$t_{i_1} \neq r_{i_1}$，因此 $|r_{i_1} - t_{i_1}| \geqslant 1 > \delta_2$，便得结论.

注释 Babai[5]已证明，可以用 L^3－运算找出一个格点 $\underline{x}$，使得对仅依赖于格的维的常数 c，满足 $\underline{x} - \underline{y} \le c \cdot l(\Gamma, \underline{y})$ 这一结果也可用于代替引理 3·5 或 3·6.

3·5 L^3－格基简化运算，实践

下面(图表 1)我们叙述在本书用于解丢番图方程的 L^3－运算的变形. 这一变形，设想只对整数进行，因此，偏离的错误完全可避免. 正如在[69]，图表 1，521 页中所述，运算中可出现非整有理数，甚至输入的都是任意整数.

图表 1. L^3－运算的变形

(A)

$d_0 := 1;$

$\underline{c}_i := \underline{b}_i;$

$\lambda_{i,j} := (\underline{b}_i, \underline{c}_j);$ ⎫ for $j = 1, \ldots, i-1;$

$\underline{c}_i := (d_j \cdot \underline{c}_i - \lambda_{i,j} \cdot \underline{c}_j)/d_{j-1}$ ⎭

$d_i := (\underline{c}_i, \underline{c}_i)/d_{i-1}$

（以上 for $i = 1, \ldots,$）

$k := 2;$

(1) perform (＊) for $i = k - 1;$

if $4 \cdot d_{k-2} \cdot d_k < 3 \cdot d_{k-1}^2 - 4 \cdot \lambda_{k,k-1}^2$ go to (2);

perform (＊) for $i = k - 2, \ldots, 1;$

if $k = n$ terminate;

$k := k + 1;$ go to (1);

(2) $\begin{pmatrix} \underline{b}_{k-1} \\ \underline{b}_k \end{pmatrix} := \begin{pmatrix} \underline{b}_k \\ \underline{b}_{k-1} \end{pmatrix};$

$$\begin{pmatrix}\mu_{k-1}\\ \mu_k\end{pmatrix} := \begin{pmatrix}\mu_k\\ \mu_{k-1}\end{pmatrix};\quad \begin{pmatrix}\underline{v}'^T_{k-1}\\ \underline{v}'^T_k\end{pmatrix} := \begin{pmatrix}\underline{v}'^T_k\\ \underline{v}'^T_{k-1}\end{pmatrix};$$

$$\begin{pmatrix}\lambda_{k-1,j}\\ \lambda_{k,j}\end{pmatrix} := \begin{pmatrix}\lambda_{k,j}\\ \lambda_{k-1,j}\end{pmatrix} \text{ for } j=1,\ldots,k-2;$$

(B) $$\begin{pmatrix}\lambda_{i,k-1}\\ \lambda_{i,k}\end{pmatrix} := \left(\lambda_{i,k-1}\cdot\begin{pmatrix}\lambda_{k,k-1}\\ d_k\end{pmatrix} + \lambda_{i,k}\cdot\begin{pmatrix}d_{k-2}\\ -\lambda_{k,k-1}\end{pmatrix}\right)/d_{k-1}$$

for $i=k+1,\ldots,n$;

(C) $d_{k-1} := (d_{k-2}\cdot d_k + \lambda^2_{k,k-1})/d_{k-1}$;

if $k>2$ then $k := k-1$;

go to (1);

(*) if $2\cdot|\lambda_{k,l}| > d_l$ then

$$\begin{cases} r := \text{integer nearest to } \lambda_{k,l}/d_l;\\ \underline{b}_k := \underline{b}_k - r\cdot\underline{b}_l;\ \mu_k := \mu_k - r\cdot\mu_l;\ \underline{v}'^T_l := \underline{v}'^T_l + r\cdot\underline{v}'^T_k;\\ \lambda_{k,j} := \lambda_{k,j} - r\cdot\lambda_{l,j} \text{ for } j=1,\ldots,l-1;\\ \lambda_{k,l} := \lambda_{k,l} - r\cdot d_l. \end{cases}$$

设 $\Gamma\in Z^n$ 是具有基向量 $\underline{b}_1,\cdots,\underline{b}_n$ 的格. 分别定义 $\underline{b}_i^*$, $\mu_{i,j}$, d_i 如文献[69](1·2),(1·3),(1·24). d_i 可作为出现在初始运算中的所有数的分母.([69]P.523).因此,对所有有关下标 i, j, 输入

$$\underline{c}_i = d_{i-1}\cdot\underline{b}_i^*$$

$$\lambda_{i,j} = d_j\cdot\mu_{i,j}. \tag{3·13}$$

由文献[69]的(1·28)和(1·29),它们都是整数.注意到满足 $B_i = |\underline{b}_i^*|^2$,

$$d_i = d_{i-1}\cdot B_i. \tag{3·14}$$

现在我们可以改写代替 $\underline{b}_i^*$, B_i, $\mu_{i,j}$的关于 $\underline{c}_i$, d_i, $\lambda_{i,j}$的运算,因

此消去所有非整有理数.我们得到这一 L^3 - 运算的变形如图表 1. 在这一变形中,除(A)、(B)、(C)各行将在下面解释之外,其余所有各行显然是应用(3·13)、(3·14),由原来运算的对应行得到的.

为了计算由原来的简化基变换来的矩阵,我们在运算时添加若干行.设 $\mathscr{B}$ 是具有为运算而输入的格 Γ 的初始基的列向量 $\underline{b}_1, \cdots, \underline{b}_n$ 的矩阵,我们说 $\mathscr{B}$ 是关于基 $\underline{b}_1, \cdots, \underline{b}_n$ 的矩阵联合.设 $\mathscr{C}$ 是关于简化基 $\underline{c}_1, \cdots, \underline{c}_n$ 的矩阵联合,其运算提供输出,则我们定义这个变换矩阵 $\mathscr{V}$ 用

$$\mathscr{C} = \mathscr{B} \cdot \mathscr{V}$$

更一般地,设 $\mathscr{U}$ 是从某个 $\mathscr{B}_0$ 到 $\mathscr{B}$ 的变换矩阵,这样,$\mathscr{B} = \mathscr{B}_0 \cdot \mathscr{U}$ 用 $\underline{u}_1, \cdots, \underline{u}_n$ 表示 $\mathscr{U}$ 的列向量,用 $\underline{v}_1^T, \cdots, \underline{v}_n^T$ 表示 $\mathscr{U}^{-1}$ 的行向量 我们也向 $\mathscr{U}$ 和 $\mathscr{U}^{-1}$ 提供运算.对 $\underline{b}_i$ 运算所做的全部处理同样用于 $\underline{u}_i$,而且 $\underline{v}_i^T$ 相应地被调整.这不影响计算时间.现在,运算给出矩阵 $\mathscr{C}$,$\mathscr{U}'$ 和 $\mathscr{U}'^{-1}$ 作为输出,使得 $\mathscr{C}$ 与简化基联合,$\mathscr{C} = \mathscr{B} \cdot \mathscr{V}$, $\mathscr{U}' = \mathscr{U} \cdot \mathscr{V}$ 注意到 $\mathscr{V}$ 没有明确地计算,除非 $\mathscr{U} = \mathscr{I}$(单位矩阵),在此情形,$\mathscr{U}' = \mathscr{V}$ 由此导出

$$\mathscr{C} = \mathscr{B} \cdot \mathscr{U}^{-1} \cdot \mathscr{U}' = \mathscr{B}_0 \cdot \mathscr{U}'$$

因此 $\mathscr{U}'$ 是从 $\mathscr{B}_0$ 到 $\mathscr{C}$ 的变换矩阵 注意到若 $\mathscr{B}$ 已知,则计算 $\mathscr{C}^{-1}$ 也不须多少额外的努力.

现在我们解释(A)、(B)、(C)各行为什么是正确的.

(A): 由文献[69](1·2)导出

$$\underline{c}_i = d_{i-1} \cdot \underline{b}_i - \sum_{k=1}^{i-1} \frac{d_{i-1}}{d_{k-1} \cdot d_k} \cdot \lambda_{i,k} \cdot \underline{c}_k$$

对 $j=0,1,\cdots,i-1$，定义

$$\underline{c}_i(j) = d_j \cdot \underline{b}_i - \sum_{k=1}^{j} \frac{d_j}{d_{k-1} \cdot d_k} \cdot \lambda_{i,k} \cdot \underline{c}_k$$

则 $\underline{c}_i(0)=\underline{b}_i$，$\underline{c}_i(i-1)=\underline{c}_i$，$\underline{c}_i(j)$恰好是在(A)中第 j 步计算出的向量，因为

$$\frac{d_j \cdot \underline{c}_i(j-1) - \lambda_{i,k} \cdot \underline{c}_j}{d_{j-1}}$$

$$= d_j \cdot \underline{b}_i - \sum_{k=1}^{i-1} \frac{d_j}{d_{k-1} \cdot d_k} \cdot \lambda_{i,k} \cdot \underline{c}_k - \frac{d_j}{d_{j-1} \cdot d_k} \cdot \lambda_{i,j} \cdot \underline{c}_j = \underline{c}_i(j),$$

这就解释了(A)中的循环公式．留下的是证明出现的向量 $\underline{c}_i(j)$是整数．这由

$$d_j \cdot \sum_{k=1}^{j} \frac{1}{d_{k-1} \cdot d_k} \cdot \lambda_{i,k} \cdot \underline{c}_k = d_j \cdot \sum_{k=1}^{j} \mu_{i,k} \cdot \underline{b}_k^*$$

导出，由文献[69]523 页 e.11，可知这是整数．

(B)，(C)：注意在原来计算中，以标记(2)开始第三和第四行是依赖于第一、第二和第五行的．这些行的这种置换是容许的．我们写出其第一、第二和第五行如下(这里，我们指出，变量已改变为原来的符号)：

$$B'_{k-1} := B_k + \mu_{k,k-1}^2 \cdot B_{k-1}; \qquad (3 \cdot 15)$$

$$B'_k := B_{k-1} \cdot B_k / B'_{k-1}; \tag{3·16}$$

$$\mu'_{k,k-1} := \mu_{k,k-1} \cdot B_{k-1} / B'_{k-1}; \tag{3·17}$$

$$\mu'_{k,k-1} := \mu'_{k,k-1} \cdot \mu_{i,k-1} + (1 - \mu_{k,k-1} \cdot \mu'_{k,k-1}) \cdot \mu_{i,k}; \tag{3·18}$$

$$\mu'_{i,k} := \mu_{i,k-1} - \mu_{k,k-1} \cdot \mu_{i,k}; \tag{3·19}$$

这里(3·18)和(3·19)对 $i = k+1, \cdots, n$ 成立. d_i 对 $i = 0, 1, \cdots, k-1$ 保持不变. 由(3·16), 也对 $i = k$ 保持不变. 现在, (3·15)等价于

$$\frac{d'_{k-1}}{d_{k-2}} = \frac{d_k}{d_{k-1}} + \frac{\lambda^2_{k,k-1}}{d^2_{k-1}} \cdot \frac{d_{k-1}}{d_{k-2}} \tag{3·20}$$

由此解释(C). 由(3·17)我们找到

$$\frac{\lambda'_{k,k-1}}{d_{k-1}} = \frac{\lambda_{k,k-1}}{d_{k-1}} \cdot \frac{d_{k-1}}{d_{k-2}} \cdot \frac{d'_{k-2}}{d'_{k-1}}$$

因此 $\lambda_{k,k-1}$ 保持不变. 由(3·18), 我们得到

$$\frac{\lambda'_{i,k-1}}{d'_{k-1}} = \frac{\lambda_{k,k-1}}{d'_{k-1}} \cdot \frac{\lambda_{i,k-1}}{d_{k-1}} + [1 - \frac{\lambda_{k,k-1}}{d_{k-1}} \cdot \frac{\lambda_{k,k-1}}{d'_{k-1}}] \cdot \frac{\lambda_{i,k}}{d_k},$$

由此, 通过乘积 $d_{k-1} \cdot d'_{k-1}$ 并利用(3·20), 有

$$d_{k-1} \cdot \lambda'_{i,k-1} = \lambda_{k,k-1}\lambda_{i,k-1} + (d_{k-1} \cdot d'_{k-1} - \lambda^2_{k,k-1}) \cdot \frac{\lambda_{i,k}}{d_k}$$

$$= \lambda_{k,k-1} \cdot \lambda_{i,k-1} + d_{k-2} \cdot \lambda_{i,k}.$$

最后，由(3·19)看出

$$\frac{\lambda'_{i,k}}{d_k} = \frac{\lambda_{i,k-1}}{d_{k-1}} - \frac{\lambda_{k,k-1}}{d_{k-1}} \cdot \frac{\lambda_{i,k}}{d_k}.$$

(B)导出.

在应用中，我们常常有一个格 Γ，其基是给定的，使得联合矩阵比如 $\mathfrak{S}$ 有着下面的特殊形式：

$$\mathfrak{S} = \begin{bmatrix} 1 & & \varnothing & \\ & \ddots & & \\ \varnothing & & 1 & \\ \theta_1 & \cdots & \theta_{n-1} & \theta_n \end{bmatrix}$$

其中 θ_i 是大整数，它可以达到数百个十进数字. 对 L^3 - 运算，运用矩阵 $\mathfrak{S}$ 自身作为输入，我们可以直接计算出这个格的简化基. 但把计算分开成能增加精确度的若干步骤，可以节省时间和空间，如下述.

设 k 是一个自然数(步骤数)，l 是一个自然数，使得 θ_i 有关于 $k \cdot l$ 的(十进)数字. 对于 $i = 1, \cdots, n$ 及 $j = 1, \cdots, k$，令

$$\theta_i^{(j)} = [\theta_i / 10^{l \cdot (k-j)}]$$

并由

$$\theta_i^{(j+1)} = 10^l \cdot \theta_i^{(j)} + \psi_i^{(j)}.$$

定义 $\psi_i^{(j)}$，因此 $\psi_i^{(j)}$ 是 l 的一组关于 θ_i 的连续数字. 对相应的 j

定义 n×n 矩阵

$$\mathfrak{S}_j = \begin{bmatrix} 1 & & & \\ & \ddots & \varnothing & \\ & \varnothing & 1 & \\ \theta_1^{(j)} & \cdots & \theta_{n-1}^{(j)} & \theta_n^{(j)} \end{bmatrix} \qquad \mathfrak{D}_j = \begin{bmatrix} & & \\ & \cdot & \\ & \varnothing & \\ \psi_1^{(j)} & \cdots & \psi_n^{(j)} \end{bmatrix}$$

$$\mathfrak{S} = \begin{bmatrix} 1 & & & \\ & \ddots & \varnothing & \\ \varnothing & & \ddots & \\ & & & 10^l \end{bmatrix}$$

则立即导出

$$\mathfrak{S}_{j-1} = \varepsilon \cdot \mathfrak{S}_j + \mathfrak{D}_j$$

注意到 $\mathfrak{S}_k = \mathfrak{S}$，因为 $\theta_i^{(k)} = \theta_i$. 令 $\mathscr{U}_0 = i$, $\mathscr{B}_1 = \mathfrak{S}_1$. 对某个 $j \geq 1$，设 $\mathscr{B}_j$ 和 $\mathscr{U}_{j-1}$是已知矩阵. 则我们运用 L^3－运算到 $\mathscr{B} = \mathscr{B}_j$, $\mathscr{U} = \mathscr{U}_{j-1}$以及 $\mathscr{U}^{-1}$，由此找到矩阵 $\mathscr{E}_j$, $\mathscr{U}_j$ 和 $\mathscr{U}_j^{-1}$，使得

$$\mathscr{E}_j = \mathscr{B}_j \cdot \mathscr{U}_{j-1}^{-1} \cdot \mathscr{U}_j$$

现在令

$$\mathscr{B}_{j+1} = \mathscr{E} \cdot \mathscr{E}_j + \mathscr{D}_j \cdot \mathscr{U}_j$$

由归纳法，$\mathscr{B}_j$, $\mathscr{E}_j$, $\mathscr{U}_j$ 对 $j = 1, \cdots, k$ 被定义. 注意

$$\mathscr{B} \cdot \mathscr{U}_j^{-1} = \mathscr{E} \cdot \mathscr{B}_j \cdot \mathscr{U}_{j-1}^{-1} + \mathscr{D}_j,$$

因此 $\mathscr{B}_j \cdot \mathscr{U}_{j-1}^{-1}$同 $\mathfrak{S}$ 一样满足相同的循环关系，因为 $\mathscr{B} \cdot \mathscr{U}_0^{-1} =$

$\mathfrak{S}_1$，我们有 $\mathscr{B}_j \cdot \mathscr{U}_{j-1}^{-1} = \mathfrak{S}_j$ 对所有 j 成立．因此

$$\mathscr{E}_j = \mathscr{B}_j \cdot \mathscr{U}_{j-1}^{-1} \cdot \mathscr{U}_j = \mathfrak{S}_j \cdot \mathscr{U}_j$$

由此导出 $\mathscr{E}_k$ 和 $\mathfrak{S}_k$ 对相同格 Γ 的基是联合的．此外，因为 $\mathscr{E}_k$ 是 L^3 - 运算的输出，它对 Γ 的简化基是联合的．

现在，让我们来分析计算时间．对矩阵 $\mathscr{M}$，我们用 $L(\mathscr{M})$ 表示其记入的（十进）数字的最大数．若 L^3 - 运算被用于矩阵 $\mathscr{B}$，正好输出一个矩阵 $\mathscr{E}$，则按照 Lenstra，Odlyzko（参阅 Lenstra[68]，P.7）和我们自己的体验，其计算时间实际上与 $L(\mathscr{B})^3$ 成比例．因为 $\mathscr{E}$ 对简化基是联合的，我们假定

$$L(\mathscr{E}) \cong {}^{10}\log(\det\Gamma)/n.$$

对我们的情形，$L(\mathfrak{S}_j) = \cong l \cdot j$，$L(\mathscr{D}_j) \cong l$，而且由于 $\det\mathscr{E} = \det\mathfrak{S}_j = \theta_n^{(j)}$，我们得到 $L(\mathscr{E}) \cong l \cdot j/n$，令 $\mathscr{E}_j = (c_{i,h}^{(j)})$，$\mathscr{U}_j(u_{i,h}^{(j)})$，则由 $\mathscr{E}_j = \mathfrak{S}_j \cdot \mathscr{U}_j$ 及 $\mathfrak{S}$ 的特别情形，有 $c_{i,h}^{(j)} = u_{i,h}^{(j)}$，$i = 1, \cdots, n-1$，$h = 1, \cdots, n$，且

$$u_{n,h}^{(j)} = [-c_{1,h}^{(j)} \cdot \theta_1^{(j)} - \cdots - c_{n-1,h}^{(j)}\theta_{n-1}^{(j)} + c_{n,h}^{(j)}]/\theta_n^{(j)}.$$

由此导出 $L(\mathscr{U}_j) \cong L(\mathscr{E}_j)$．因此

$$L(\mathscr{B}_j) \cong \max[L(\mathscr{E} \cdot \mathscr{E}_{j-1}), L(\mathscr{D}_{j-1} \cdot \mathscr{U}_{j-1})] \cong l + l \cdot (j-1)/n.$$

将 $\mathfrak{S}$ 作为输入代替运用一次 L^3 运算，我们将 $\mathscr{B}_1, \cdots, \mathscr{B}_k$ 作为输入，应用 k 次，由此，通过因子

$$\frac{L(\mathfrak{S})^3}{\sum_{j=1}^{k} L(\mathscr{B}_j)^3} \cong \frac{(l\cdot k)^3}{\sum_{j=1}^{k} l^3\cdot(1+\frac{j-1}{n})^3} = \frac{k^3\cdot n^3}{\sum_{j=0}^{k-1}(n+j)^3}$$

减少了计算时间. 对于 $2\cdot5\cdot n$ 与 $3\cdot n$ 之间的 k, 这个表达式最大, 大约 $0.4\cdot n^2$. 因此, 计算时间上的节省是能考虑的(一个因子 10 已当作 $n=5$). 所需的存储器空间也可节省, 因为出现在输入中的最大数 $l\cdot[1+(k-1)n]$ 已被 $l\cdot k$ 数字代替.

3·6 寻找所有短格点:Fincke 和 Pohst 运算

有时仅有关于 $l(\Gamma)$ 或 $l(\Gamma, \underline{y})$ 的下界是不够的. 对于给定常数 C, 确切知道所有向量 $\underline{x}\in\Gamma$ 使得 $|\underline{x}|\leqslant C$ 或 $|\underline{x}-\underline{y}|\leqslant C$ 是有益的. 存在着找出这些问题的所有解的有效运算. 这一运算已被 Fincke 和 Pohst[43]提出. 参阅他们的(2·8)和(2·12). 我们给出这一运算的叙述如下.

运算的输入是其列向量使格 Γ 旋转的一个矩阵 $\mathscr{B}$ 以及一个常数 $C>0$. 输出是列出所有满足 $|\underline{x}|\leqslant C$ 的格点 $\underline{x}\in\Gamma$, 除去 $\underline{x}=0$ 之外. 我们给出此运算如图表 2. 我们用 $\mathscr{X}=(x_{ij})$ 表示矩阵 $\mathscr{X}=\mathfrak{S}, \mathscr{B}, \mathscr{R}, \varphi, \mathfrak{U}$, 而 $\underline{x}_i$ 表示 $\mathscr{X}$ 的列向量.

图表 2. Fincke 和 Pohst 运算

$\mathfrak{S} := \mathscr{B}^T\cdot\mathscr{B}$;

$q_{ij} := a_{ij}$ for $1\leqslant i\leqslant j\leqslant n$;

$q_{ji} := q_{ij}$, $q_{ij} := q_{ij}/q_{ii}$ for $1 \leqslant i < j \leqslant n$;

$q_{kl} := q_{kl} - q_{ki} \cdot q_{il}$ for $i+1 \leqslant k \leqslant l \leqslant n$ for $1 \leqslant i \leqslant n$;

$r_{ii} := \sqrt{q_{ii}}$ for $1 \leqslant i \leqslant n$;

$r_{ij} := r_{ii} \cdot q_{ij}$, $r_{ji} := 0$ for $1 \leqslant j < i \leqslant n$;

compute $\mathcal{R}^{-1}$;

compute a row − reduced version φ^{-1} of $\mathcal{R}^{-1}$, and $\mathcal{U}$, $\mathcal{U}^{-1}$ such that $\varphi^{-1} = \mathcal{U}^{-1} \cdot \mathcal{R}^{-1}$;

compute $\varphi = \mathcal{R} \cdot \mathcal{U}$;

determine a permutation π such that $|\underline{s}_{\pi(1)}| \geqslant \ldots \geqslant |\underline{s}_{\pi(n)}|$, let φ' be the matrix wich columns $\underline{s}_{\pi^{-1}(i)}$ for $i = 1, \ldots, n$;

$\mathfrak{S} := \varphi'^{T} \cdot \varphi'$;

$q_{ij} := a_{ij}$ for $1 \leqslant i \leqslant j \leqslant n$;

$q_{ji} := q_{ij}$, $q_{ij} := q_{ij}/q_{ii}$ for $1 \leqslant i < j \leqslant n$;

$q_{kl} := q_{kl} - q_{ki} \cdot q_{il}$ for $i+1 \leqslant k \leqslant l \leqslant n$ for $1 \leqslant i \leqslant n$;

$i := n$;

$T_i := c$;

$U_i := 0$;

(1) $Z := /(T_i/q_{ii})$;

$UB(x_i) := [Z - U_i]$;

$x_i := [-Z - U_i] - 1$;

(2) $x_i := x_i + 1$;

if $x_i \leqslant UB(x_i)$, go to (4);

(3) $i := i + 1$;

go to (2);

(4) if $i = 1$, go to (5);

$i := i - 1$;

$U_i := \sum_{j=i+1}^{m} q_{ij} \cdot x_j$;

$T_i := T_{i+1} - q_{i+1,i+1} \cdot (x_{i+1} + U_{i+1})^2$;

go to (1);

(5) if $x_i = 0$ for $1 \leqslant i \leqslant n$, terminate;

compute and print $\underline{x} = \mathcal{U} \cdot (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})^T$;

go to (2).

此运算也可用于找出所有向量 $\underline{x} \in \Gamma$, $\underline{x}$ 到给出的非格点 $\underline{y}$ 的距离至多是一给定常数 C. 即是说，设

$$\underline{y} = \sum_{i=1}^{n} s_i \cdot \underline{b}_i .$$

又设对所有 i, r_i 是最接近 s_i 的整数. 设

$$\underline{z} = \sum_{i=1}^{n} r_i \cdot \underline{b}_i$$

则 $|\underline{y} - \underline{z}| < C'$ 对某常数 C' 成立.($C' = \frac{n}{2} \cdot \sum |\underline{b}_i|$ 将算出). 因为 $\underline{z} \in \Gamma$, 足以检查所有满足 $|\underline{u}| \leqslant C + C'$ 的格点 $\underline{u}$ 并对每一个这样的格点 $\underline{u}$ 也可计算 $\underline{x} = \underline{z} + \underline{u}$, 因为 $|\underline{x} - \underline{y}| < C$ 蕴涵

$$|\underline{u}| \leqslant |\underline{x} - \underline{y}| + |\underline{y} - \underline{z}| \leqslant C + C'$$

3·7 实情形的齐次多维逼近:实逼近格点

设线性型 Λ 形如

$$\Lambda = \sum_{i=1}^{n} x_i \cdot \theta_i$$

我们假定 $n \geqslant 2$. $n = 2$ 的情形已在 3·2 节中讨论, 但本节所用

的方法也适合于 $n=2$. 事实上，在这一情形，其方法在本质上是相同的.

设 C 是足够大的整数，其数值的大小是 X_0^n. 设 $\gamma\in N$ 是常数(后面将解释其用途). 我们用矩阵

$$\mathscr{B}=\begin{bmatrix} \gamma & & & \\ & \ddots & \varnothing & \\ \varnothing & & \gamma & \\ [\gamma\cdot C\cdot\theta_1] & \cdots & [\gamma\cdot C\cdot\theta_{n-1}] & [\gamma\cdot C\cdot\theta n] \end{bmatrix}$$

定义逼近格 Γ，其列向量 $\underline{b}_1,\cdots,\underline{b}_n$ 是格的基. 则 Γ 是行列式为 $\gamma^{n-1}\cdot[\gamma\cdot C\cdot\theta_n]$的 Z^n 的子格，其大小为 C. 格点 $\underline{x}$ 形如

$$\underline{x}=\sum_{i=1}^{n}x_i\cdot\underline{b}_i=[\gamma\cdot x_1,\cdots,\gamma\cdot x_{n-1},\widetilde{\Lambda}]^T$$

其中 x_i 是整数，且

$$\widetilde{\Lambda}=\sum_{i=1}^{n}x_i\cdot[r\cdot C\cdot\theta_i].$$

显然，$\widetilde{\Lambda}$ 靠近于 $r\cdot C\cdot\Lambda$. 向量 $\underline{x}$ 的长在 X_0 与 $|\Lambda|$ 的范围内. 为确定起见，我们想将这两个数中一个与另一个作比较. Heuristics(参阅 1·3 节)告诉我们，在一般情形下我们要求 $|\Lambda|\cong X_0^{-n}$. 现在我们容易证明下面有用的引理.

引理 3·7　设 X_1 是一个正数，使得

$$l(\Gamma)\geqslant\sqrt{(n+1)^2+(n-1)\cdot r^2}\cdot X_1 \tag{3·21}$$

则(3·1)没有满足

$$\frac{1}{\delta}\cdot\log(r\cdot C\cdot c/X_1)\leqslant X\leqslant X_1 \tag{3·22}$$

的解.

注:我们对 $X_1=X_0$ 应用这一引理.若此时条件(3·21)舍弃,我们必须取一个较大的常数 C.若它对大小为 X_0^n 的常数 C 成立,则(3·22)对大小为 $\log X_0$ 的 X 导出一个降低的下界.

证明 设 $x_1,\cdots,x_n$ 是(3·1)的满足 $0<X<X_1$ 的解.考虑格点

$$\underline{x}=\sum_{i=1}^{n}x_i\cdot\underline{b}_i=[r\cdot x_1,\cdots,r\cdot x_{n-1},\widetilde{\Lambda}]^T$$

其中 $\widetilde{\Lambda}$ 如上所述.则

$$|\underline{x}|^2=\gamma^2\cdot\sum_{i=1}^{n-1}x_i^2+\widetilde{\Lambda}^2\leqslant(n-1)\cdot\gamma^2\cdot x_1^2+\widetilde{\Lambda}^2$$

且

$$|\widetilde{\Lambda}-\gamma\cdot C\cdot\Lambda|\leqslant\sum_{i=1}^{n}|x_i|\cdot|[\gamma\cdot C\cdot\theta_i]-\gamma\cdot C\cdot\theta_i|\leqslant\sum_{i=1}^{n}|x_i| \tag{3·23}$$

此必 $\leqslant n\cdot X_1$.由(3·1),(3·21)及 $l(\Gamma)$ 的定义,有

$$\gamma\cdot C\cdot c\cdot \exp(-\delta\cdot X)>|\gamma\cdot C\cdot \Lambda|\geqslant$$

$$|\widetilde{\Lambda}|-|\breve{\Lambda}-\gamma\cdot C\cdot \Lambda|\geqslant$$

$$\geqslant\sqrt{l(\Gamma)^2-(n-1)\cdot\gamma^2\cdot X_1^2}-n\cdot X_1\geqslant X_1.$$

由此立得(3·22).

条件(3·21)可应用 L^3－运算通过计算格 Γ 的简化基来检验，而运用引理 3·4，应用参数 γ 使"偏离的错误"

$$|[\gamma\cdot C\cdot\theta_i]-\gamma\cdot C\cdot\theta_i|.$$

相对地小. 这仅当 C 不是很大时才是重要的，通常仅在已完成第一步骤之后，若想进行进一步简化步骤时. 对大 C，简单地取 $\gamma=1$.

若 C 不是很大，应用更精炼的方法来降低上界是必要的. 为此，我们应用下面引理，此引理是引理 3·7 同 Fincke 和 Pohst 运算(参阅 3·6 节)稍为优美的结合. 这对于 $|x_i|$ 当 i 不同时有不同上界的情况特别有用.

引理 3·8　假定对(3·1)的解

$$|\widetilde{\Lambda}|>\sum_{i=1}^{n}|x_i| \tag{3·24}$$

成立，则

$$X<\frac{1}{\delta}\cdot\log[r\cdot C\cdot c/[|\widetilde{\Lambda}|-\sum_{i=1}^{n}|x_i|]] \tag{3·25}$$

证明　格点 $\underline{x}$ 的定义如同引理 3·7 的证明. 由(3·23)和

(3·24)

$$|\Lambda|\geqslant[|\widetilde{\Lambda}|-\sum_{i=1}^{n}|x_i|]/\gamma\cdot C>0.$$

由(3·1)即得结论.

我们继续进行如下.选择一常数 C_0 使得当 $|\widetilde{\Lambda}|>C_0$ 时,则 $|x_i|$ 的上界蕴涵在(3·24).在此情形,从(3·25),我们有关于 X 的一个新上界.在 $|\widetilde{\Lambda}|\leqslant C_0$ 的情形,我们有关于向量 x 的长度的一个上界.我们用 Fincke 和 Pohst 运算计算满足这个界的所有格点,并对(3·1)检验它们.

概言之,上面介绍的简化方法基于这样的事实,就是(3·1)的大解对应于在适当的逼近格中的一个极端短的向量.因为我们可以通过计算实际证明这样的短向量不存在,由此导出这样的大解不存在,我们将在第五章中应用这些技巧.

3·8 实情形的非齐次多维逼近:对推广的 Davenport 引理的一种取舍

设 Λ 是我们要研究的最一般线性型,即

$$\Lambda=\beta+\sum_{i=1}^{n}x_i\cdot\theta_i.$$

其中 n≥2(n=2 的情形已在 3·3 节中论及,但这里也可结合起来).为论及这种非齐次情形,有两种方法可使用.第一种方法是我们在 3·3 节中讨论的 Davenport 方法的推广.第 2 种

方法接近前节的齐次情形.

首先我们简扼解释推广的 Davenport 方法. 参阅 Ellison [36](其中只对 $n=3$ 的情形). 设

$$\theta'_i=\theta_i/\theta_n,\quad i=1,\cdots,n-1,\quad \beta'=\beta/\theta_n.$$

$$\Lambda'=\Lambda/\theta_n=\beta'+\sum_{i=1}^{n-1}x_i\cdot\theta_i'+x_n$$

设$(p_1,\cdots,p_{n-1},q)$联立逼近 $\theta_1',\cdots,\theta'_{n-1}$, 其中 q 的大小为 X_0^{n-1}, 使得当 $i=1,\cdots,n-1$ 时

$$|\theta_i'-p_i/q|<c'/q^{1+1/(n-1)}$$

对一个小的常数 C' 成立.

引理 3·9(Davenport, Ellison) 假定

$$\|q\cdot\beta'\|>2\cdot(n-1)\cdot X_0\cdot C'/q^{1/(n-1)}.$$

则(3·1)和(3·2)的解满足

$$X<\frac{1}{\delta}\cdot\log[q^{1+1/(n-1)}\cdot c/|\theta_n|\cdot c'\cdot(n-1)\cdot X_0].$$

证明 由

$$\|q\cdot\beta'\|\leqslant|q\cdot\Lambda'+\sum_{i=1}^{n-1}x_i\cdot(p-q_i\theta_i')|$$
$$\leqslant q\cdot|\theta_n|^{-1}\cdot c\cdot\exp(-\delta\cdot X)+(n-1)\cdot X_0\cdot c'/q^{1/(n-1)}$$

立得结论.

实际应用这个一般的 Davenport 方法计算联立逼近$(p_1,\cdots,p_{n-1},q)$是必要的. 我们在 1·4 节指出了这为什么能运用

L^3－运算来进行. 作为格我们取下面矩阵的一个联合：

$$\begin{bmatrix} 1 & & & \\ [C\cdot\theta'_1] & -C & & \varnothing \\ \cdots & & \ddots & \\ & \varnothing & & \\ [C\cdot\theta'_{n-1}] & & & -C \end{bmatrix}.$$

其中 C 是大小为 X_0^n 的常数. 则 $\underline{c}_1$ 是简化基的第一个基向量，其长度的大小 $C^{(n-1)/n} \cong X_0^{n-1}$. 但 $\underline{c}_1$ 可写成

$$\underline{c}_1 = [q, q\cdot[C\cdot\theta_1'] - Cp_1, \cdots, q\cdot[C\cdot\theta_{n-1}'] - Cp_{n-1}]^T$$

对某 $p, \cdots, p_{n-1}, q$. 要求 q 的大小是 X_0^{n-1}, 且

$$q\cdot C\cdot|\theta_i' - p_i/q| \cong |q\cdot[C\cdot\theta_i'] - C\cdot p_i|$$

的大小为 X_0^{n-1}. 因此 $|\theta_i' - p_i/q|$ 的大小为

$$X_0^{n-1}/C\cdot X_0^{n-1} = C^{-1} \cong X_0^{-n} \cong q^{-(1+1/(n-1))}.$$

此为所求.

上述方法已被实际用于解 Thue 和 Thue－Mahler 方程，作者有 Agrawal, Coates, Hunt 和 Van der Poorth[1]（运用多维连分数代替 L^3－运算），还有 Pethö, Schulenberg[92]、Blass, Glass, Meronk 和 Steiner[16], [17]. 因此，已证明是有效的. 然而，我们介绍另一方法，有几个理由. 首先，正如前节所述，它接近于齐次的情形，而一般的 Davenport 方法没有明显的配对方法用于齐次情形. 第二、它实际产生的解对于线性型 Λ 来说在 $X \leqslant X_0$ 的条件下可能几乎接近于零. 特别地，若在 θ_i 之间存在线性关系，而以前没有指明这一点（实际上可

能发生这种情况，参阅 Agrawal, Coates, Hunt 和 Van der Poorten[1]).发现这些关系的方法是通过给出关系系数找到极短的格向量(各格向量极端接近于给定点).第三、对 p-adic 情形的模似方法也可给出(看 3·11 节).最后，正如 1·4 节指出的，变换是可能的.关于计算时间，我们认为两种方法速度是相当的.

此方法步骤如下.我们恰如齐次的情形取逼近格 Γ(参阅前节)，满足适当选择的常数 r, C，即 C 的大小是 X_0^n. 用 L^3-运算计算 Γ 的简化基 $\underline{c}_1, \cdots, \underline{c}_n$. 设 $\mathfrak{C}$ 是此基的矩阵联合，同时也计算满足 $\mathfrak{C}=\mathfrak{B}\cdot\mathfrak{U}$ 的变换矩阵 $\mathfrak{U}$ 及其逆 $\mathfrak{U}^{-1}$. 注意到 $\mathfrak{B}^{-1}$ 以及由此也有 $\mathfrak{C}$ 是易于计算的，即由

$$\mathfrak{B}^{-1}=\begin{bmatrix} 1/r & & & \\ & \ddots & & \emptyset \\ & \emptyset & 1/r & \\ -\dfrac{[r\cdot C\cdot\theta_1]}{r\cdot[r\cdot C\cdot\theta_n]} & \cdots & -\dfrac{[r\cdot C\cdot\theta_{n-1}]}{r\cdot[r\cdot C\cdot\theta_n]} & \dfrac{1}{[r\cdot C\cdot\theta_n]} \end{bmatrix}$$

及 L^3-运算的变形(图表 1)而算出.设 $\underline{y}\in Z^n$，由

$$\underline{y}=[0,\cdots,0,-[r\cdot C\cdot\beta]]^T=\sum_{i=1}^{n}s_i\cdot\underline{c}_i$$

定义，其中系数 $s_i\in R$ 可由

$$[s_1,\cdots,s_n]^T=\mathfrak{C}^{-1}\cdot\underline{y}$$

计算.为了更精确起见，若 $\mathfrak{U}^{-1}$ 以 $\underline{u}$ 作为第 n 列，则 $\mathfrak{C}^{-1}$ 以 $\underline{u}/[r\cdot C\cdot\theta_n]$ 作为第 n 列.因此

$$[s_1,\cdots,s_n]^T=-\underline{u}[r\cdot C\cdot\beta]/[r\cdot C\cdot\theta_n].$$

现在我们应用引理 3·5 或 3·6，得到 $l(\Gamma, \underline{y})$ 的一个下界. 因此我们可应用下面引理.

引理 3·10　设 X_1 是一个正常数使得

$$l(\Gamma, \underline{y}) \geqslant \sqrt{(n+2)^2 + (n-1)r^2} \cdot X_1. \tag{3·26}$$

则(3·1)没有满足

$$\frac{1}{\delta} \cdot \log(r \cdot C \cdot c / X_1) \leqslant X \leqslant X_1 \tag{3·27}$$

的解.

注：对 $X_1 = X_0$ 应用这个引理. 若条件(3·26)不具备，我们需取一个较大的常数 C. 若它对大小为 X_0^2 的常数 C 成立，则(3·27)导出 X 降低的下界，其大小为 $\log X_0$.

证明　设 $x_1, \cdots, x_n$ 是(3·1)满足 $0 < X < X_1$ 的解. 考虑格点

$$\underline{x} = \sum_{i=1}^{n} x_i \cdot \underline{b}_i = [r \cdot x_1, \cdots, r \cdot x_{n-1}, \widetilde{\Lambda}_0]^T,$$

其中 $\widetilde{\Lambda}_0 = \sum_{i=1}^{n} x_i \cdot [r \cdot C \cdot \theta_i]$. 设 $\widetilde{\Lambda} = [r \cdot C \cdot \beta] + \widetilde{\Lambda}_0$，则

$$|\underline{x} - \underline{y}|^2 = r^2 \cdot \sum_{i=1}^{n-1} x_i^2 + \widetilde{\Lambda}^2 \leqslant (n-1) r^2 \cdot X_1^2 + \widetilde{\Lambda}^2,$$

且

$$|\widetilde{\Lambda} - r \cdot C \cdot \Lambda| \leqslant |[r \cdot C \cdot \beta] - r \cdot C \cdot \beta| + \sum_{i=1}^{n} |x_i| \cdot |[r \cdot C \cdot \theta_i] - r \cdot C \cdot \theta_i| \leqslant$$

$$\leqslant 1+\sum_{i=1}^{n}|x_i|\leqslant 1+nX_1\leqslant (n+1)\cdot X_1.$$

由(3·1),(3·26)及$l(\Gamma,y)$的定义便可导出结果,这是因为

$$r\cdot C\cdot c\exp(-\delta\cdot X)>|r\cdot C\cdot\Lambda|\geqslant|\widetilde{\Lambda}|-|\widetilde{\Lambda}-r\cdot C\cdot\Lambda|$$
$$\geqslant\sqrt{\iota(\Gamma,y)^2-(n-1)\cdot r^2\cdot X_1^2}-(n+1)X_1\geqslant X_1.$$

类似于在引理3·8中的齐次情形,上面引理的证明也可更简炼.我们在3·5节已说明怎样运用Fincke和Pohst运算于非齐次情形.这里我们不再进行.

概言之,上面所述的方法基于这样的事实,就是在非齐次情形,(3·1)的一个大解导出非常接近Z^n中一个定点的一个格点.我们实际上可通过某些计算证明这样的格点不存在,因此这样的极端解不存在.本节列示的方法将在第八章中应用.注意$n=2$的情形,此种方法本质上与Davenport引理相同.

3·9 p−adic 情形的非齐次零维逼近

在p−adic情形,我们从非常简单的线性型Λ开始,对此也有很简单的简化方法可应用.设Λ是

$$\Lambda=\beta+x\theta,$$

对$\beta,\theta\in\Omega_p$,使得$\beta/\theta\in Q_p$,且$x\in Z$, $x>0$.显然,在实的情形满足这一简单线性型Λ的不等式(3·1)仅有有限多个解(我们甚至不需要(3·2)),这些解容易算出.然而在p−adic情形,不

等式(3·3)可有无限多个解,因此需要一个界对(3·4),而且需要一种简化方法.

设 $\theta' = -\beta/\theta$, 则 $\theta' \in Q_p$. 不等式(3·3)变成

$$\mathrm{ord}_p(\theta' - x) \geqslant c_1{}' + c_2 \cdot x \tag{3·28}$$

其中 $c_1{}'$, c_2 是满足 $c_2 > 0$ 的常数, 我们假定

$$x \geqslant -c_1{}'/c_2$$

则当 $\mathrm{ord}_p(\theta') < 0$ 时(3·28)没有解. 因此我们可假定 θ' 是一个 p-adic 整数. 设 θ' 的 p-adic 展式是

$$\theta' = \sum_{i=0}^{\infty} u_i \cdot p^i,$$

其中 $u_i \in \{0, 1, \cdots, p-1\}$, 所有 $i \in N_0$. 计算 p-adic 数字 u_i 应用下面简化引理已经很足够了.

引理 3·11　设 X_1 是一个正常数, r 是使得

$$p^r > X_1, \quad u_r \neq 0 \tag{3·29}$$

的最小下标, 则(3·28)没有满足

$$(r - c_1{}')/c_2 < x \leqslant X_1 \tag{3·30}$$

的解.

注: 我们应用引理满足 $X_1 = X_0$. 引理后面的假设是: 在 θ' 的 p-adic 展式中不出现长的零序列. 事实上, 在我们的应用中, 数 u_i 几乎是随机地分布在 $\{0, 1, \cdots, p-1\}$ 上. 则满足(3·29)的最小的 r 将不比 $\log X_0/\log p$ 大多少, 由此, (3·30)导出

一个大小为 $\log X_0$ 的简化上界，此合符要求.

证明　设 $x \leqslant X_1$ 满足(3·28)，假定 $\mathrm{ord}_p(\theta' - x) \geqslant r+1$，则

$$x \equiv \sum_{i=0}^{r} u_i \cdot p^i \pmod{p^{r+1}}.$$

由 $x \geqslant 0$，从(3·29)导出

$$x \geqslant \sum_{i=0}^{r} u_i \cdot p^i \geqslant u_r \cdot p^r \geqslant p^r > X_1.$$

这与假设 $x \leqslant X_1$ 矛盾. 因此 $\mathrm{ord}_p(\theta' - x) \leqslant r$，由(3·28)便导出(3·30).

注：在上面证明中，本质是 $x \geqslant 0$. 然而，用公式表示类似的结果对所有 $x \in Z$ 成立也没有什么困难，由观察，若 $p \neq 2$，p-adic 数字 u_i 不仅 $\neq 0$，而且 $\neq p-1$，若 $p=2$，p-adic 数字 u_i，u_{i+1} 满足 $u_i \neq u_{i+1}$.

上面叙述的很类似的方法已被 Wagstaff[129]，[130]运用，如解 $5^n = 2 \pmod{3^n}$ 等等. 我们在第四章应用此方法.

3·10　p-adic 情形的齐次一维逼近：p-adic 连分数及 p-adic 数的逼近格

设 Λ 形如

$$\Lambda = x_1\theta_1 + x_1\theta_2.$$

其中 $\theta_1, \theta_2 \in \Omega_p$ 使得 $\theta = -\theta_1/\theta_2 \in Q_p$，$x_1, x_2 \in Z$. 我们可假定

$\mathrm{ord}_p(\theta)\geqslant 0$. 现在

$$\Lambda' = \Lambda/\theta_1 = -x_1\cdot\theta + x_2.$$

因此现在(3·3)意味着有理数 x_2/x_1 很好地逼近于 p-adic 数 θ.

类似于实的情形来研究 p-adic 连分数运算似乎是合情合理的. 然而,提供所有最好的逼近于一个 p-adic 数的 p-adic 连分数运算似乎是不存在. 因此我们引入 p-adic 逼近格的概念,这已由 de Weger 所述[134]. 本文采用最好的逼近运算,这是 Mahler[76]第四章中所述运算的推广. 这一运算背离欧几里得运算,因此是趋于连分数运算,但是在 p-adic 数表示为连分数的意义下,它不是 p-adic 连分数运算. 其逼近是在连分数截尾之后得到.

回顾对于 $\mu\in N_0$,有理数 $\theta^{(\mu)}$ 用 $\mathrm{ord}_p(\theta-\theta^{(\mu)})\geqslant\mu$ 且 $0\leqslant\theta^{(\mu)}<p^\mu$ 来定义. 对任意 $\mu\in N_0$,我们用其 Γ_μ 的基是联合的矩阵来定义 p-adic 逼近格 Γ_μ,即矩阵

$$\begin{pmatrix} 1 & 0 \\ \theta^{(\mu)} & p^\mu \end{pmatrix}.$$

则容易看出

$$\Gamma_\mu = \{[x_1, x_2]^T\in Z^2 \mid \mathrm{ord}_p(x_2 - x_1\cdot\theta)\geqslant\mu\}$$

(参阅下节引理 3·13),那里证明更一般的结果). 下面运算计算出 Γ_μ 中最小长度的点.

图表 3. p－adic 逼近运算：

```
    x: = [1, θ^μ]^T;   y: = [0, p^μ]^T;
    if |x| > |y|, interchange x and y;
(1) compute K ∈ Z such that |y − K·x| is minimal;
    y: = y − K·x;
    if |x| > |y|, interchange x and y, and go to (1);
    print x.
```

由此运算清晰地求出 $l(\Gamma_\mu)$ 是可能的. 因此, 我们可应用下面引理.

引理 3·12　设 X_1 是一个常数, 使得

$$l(\Gamma_\mu) > \sqrt{2}\cdot X_1.$$

则(3·3)没有满足

$$[\mu - 1 - c_1 + \mathrm{ord}_p(\theta_2)]/c_2 < x_j \leqslant X \leqslant X_1 \qquad (3\cdot 32)$$

的解.

注：我们取 μ 使得 p^μ 的大小是 X_0^2, 并对 $X_1 = X_0$ 应用引理, 则我们要求 $l(\Gamma_\mu)$ 的大小是 X_0, 则(3·31)是一个合适的条件.

证明　对 n = 2 运用引理 3·14(见下节)的证明便可.

类似上面所述方法已被 Agrawal, Coates; Hunt 和 Van der Poorten[1]应用, 我们将在第六章和第七章应用.

3·11 p－adic 情形的齐次多维逼近：p－adic 逼近格

现在研究

$$\Lambda = \sum_{i=1}^{n} x_i \cdot \theta_i$$

的情形，其中对所有 i，j，$\theta_i \in \Omega_p$，使得 $\theta_i/\theta_j \in Q_p$，$x_i \in Z$，并满足 $n \geqslant 2$. 我们可假定 $i=n$ 时 $\mathrm{ord}_p(\theta_i)$ 最小，设

$$\theta_i' = -\theta_i/\theta_n, \quad i=1,\cdots,n-1,$$

则对所有 i，$\theta_i' \in Z_p$. 令

$$\Lambda' = \Lambda/\theta_n = -\sum_{i=1}^{n-1} x_i \cdot \theta_i' + x_n$$

p－adic 逼近格的定义可由一维的情形直接推广. 即对任意 $\mu \in N_0$，定义 Γ_μ 为格对矩阵

$$\mathscr{B}_\mu = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ \theta_1'^{(\mu)} & \cdots & \theta_{n-1}'^{(\mu)} & p^\mu \end{bmatrix},$$

的联合. 则有下面结果：

引理 3·13 与上面定义的矩 $\mathscr{B}_\mu$ 联合的格 Γ_μ 等于集

$$\Gamma_\mu = \{(x_1, \cdots, x_n)^T \in Z^n \mid \mathrm{ord}_p(\Lambda') \geqslant \mu\}.$$

证明　对任意 $\underline{x} \in [x_1, \cdots, x_n]^T \in \Gamma_\mu$，存在着一个 $\underline{z} = [z_1, \cdots, z_n]^T \in Z^n$，使得 $\underline{x} = \mathscr{B}_\mu \cdot \underline{z}$. 则 $x_i = z_i$，$(i = 1, \cdots, n-1)$，且

$$x_n = \sum_{i=1}^{n-1} z_i \cdot \theta_i'^{(\mu)} + z_n \cdot p^\mu \equiv \sum_{i=1}^{n-1} x_i \cdot \theta_i' \pmod{p^\mu}.$$

因此 $\mathrm{ord}_p(\Lambda') \geqslant \mu$. 反之，对任意 $\underline{x} = [x_1, \cdots, x_n]^T$，满足 $\mathrm{ord}_p(\Lambda') \geqslant \mu$，显然存在一个 $\underline{z} \in Z^n$，使得 $\underline{x} = \mathscr{B} \cdot \underline{z}$.

用 L^3 - 运算，我们可计算 $l(\Gamma_\mu)$ 的下界. 则我们应用下面引理，它是引理 3·12 的直接推广.

引理 3·14　设 X_1 是常数，使得

$$l(\Gamma_\mu) > \sqrt{n} \cdot X_1 \tag{3·33}$$

则(3·3)没有满足

$$[\mu - 1 - c_1 - \mathrm{ord}_p(\theta_n)]/c_2 < x_j \leqslant X \leqslant X_1 \tag{3·34}$$

的解.

注：取 μ 使 p^μ 的大小是 X_0^n，对 $X_1 = X_0$ 应用引理. 则我们要求 $l(\Gamma_\mu)$ 的大小是 X_0，因此(3·33)是合适的条件.

证明　设 $x_1, \cdots, x_n$ 是(3·3)满足 $X \leqslant X_1$ 的解，则(3·33)不容许点 $[x_1, \cdots, x_n]^T$ 进入 Γ_μ 中的格点. 因此由(3·13)，$\mathrm{ord}_p(\Lambda') \leqslant \mu - 1$，由(3·3)便推出(3·34).

我们将在第六、第七章应用本节的结果.

3·12 p－adic 情形的非齐次一维及多维逼近

最后，我们研究非齐次 p－adic 型

$$\Lambda = \beta + \sum_{i=1}^{n} x_i \cdot \theta_i.$$

其中 $\beta, \theta_i \in \Omega_p$，使得对所有 i，j，$\beta/\theta_j, \theta_i/\theta_j \in Q_p$ 且 $x_i \in Z$，$n \geqslant 2$ 假定对 $i = n$，$\mathrm{ord}_p(\theta_i)$最小，且 $\mathrm{ord}_p(\beta) \geqslant \mathrm{ord}_p(\theta_n)$．设

$$\theta_i' = -\theta_i/\theta_n, \quad i = 1, \cdots, n-1, \quad \beta' = \beta/\theta_n,$$

$$\Lambda' = \Lambda/\theta_n = \beta' - \sum_{i=1}^{n-1} x_i \cdot \theta_i' + x_n$$

则对所有 i，$\beta', \theta_i' \in Z_p$．如同对齐次情形的定义，我们取格 Γ_μ 作为 p－adic 逼近格，即对任意 $\mu \in N_0$，格 Γ_μ 是对矩阵 A_μ 的联合（看 3·11 节），进而，设

$$y = [0, \cdots, 0, \beta'^{(\mu)}]^T = \sum_{i=1}^{n} s_i \cdot \underline{c}_i \in Z^n.$$

其中 $\underline{c}_1, \cdots, \underline{c}_n$ 是 Γ_μ 的简化基，且 $s_i \in R$．由引理 3·5 或 3·6，我们可求出 $l(\Gamma, y)$的下界．这使我们看到了下面引理的实用．

引理 3·15　集 $\Gamma_\mu(y) = \Gamma_\mu + y$ 等于集

$$\Gamma_\mu(y) = \{[x_1, \cdots x_n]^T \in Z^n \mid \mathrm{ord}_p(\Lambda') \geqslant \mu\}.$$

证明　设 $x = [x_1, \cdots, x_n]^T$ 满足 $\underline{x} - \underline{y} \in \Gamma_\mu$．注意到

$$\underline{x}-\underline{y}=[x_1,\cdots,x_{n-1},x_n-\beta'^{(\mu)}]^T$$

由引理 3·13 得到

$$\mathrm{ord}_p[\sum_{i=1}^{n-1}x_i\cdot\theta_i-(x_n-\beta'^{(\mu)})]\geqslant p^{\mu}.$$

左边恰好是 $\mathrm{ord}_p(\Lambda')$. 引理得证.

显然, $\Gamma_\mu(\underline{y})$(一个变换格)中最短向量的长等于 $l(\Gamma_\mu,\underline{y})$(除情形 $\underline{y}\in\Gamma_\mu$ 外, 即对所有 i, 有 $s_i\in Z$). 我们得到下面有用的引理.

引理 3·16. 设 X_1 是常数使得

$$l(\Gamma_\mu,\underline{y})>\sqrt{n}\cdot X_1 \tag{3·35}$$

则(3·3)没有满足

$$[\mu-1-c_1+\mathrm{ord}_p(\theta_n)]/c_2<x_j\leqslant X\leqslant X_1 \tag{3·36}$$

的解.

注: 取 μ 使得 p^μ 的大小是 X_0^n, 对 $X_0=X_1$ 应用引理, 则我们要求 $l(\Gamma_\mu,\underline{y})$ 大小是 X_0, 因此(3·35)是合适的条件.

证明 设 $x_1,\cdots,x_n$ 是(3·3)满足 $X\leqslant X_1$ 的解, 则(3·35)不容许点 $[x_1,\cdots,x_n]^T$ 进入 $\Gamma_\mu(\underline{y})$. 因此, 由引理 3·15, $\mathrm{ord}_p(\Lambda')\leqslant\mu-1$. 由(3·3)便导出(3·36).

我们在本书中将不使用这个引理, 将它包含在这里是为了完整起见. 然而, 当我们要解 Thue－Mahler 方程(见第八章第 6 节)时, 将会用到.

3·13　p－adic 逼近格的有用子格

在我们经由线性型解丢番图方程的 p－adic 应用中，我们总有代数数对数线性型，即在

$$\Lambda = \beta + \sum_{i=1}^{n} x_i \cdot \theta_i$$

中，β 和 $\theta'_i s$ 是 p－adic 代数数对数，例如

$$\beta = \log_p(\alpha_0), \quad \theta_i = \log_p(\alpha_i), \quad i = 1, \cdots, n.$$

在 2·3 节我们已看出，对 $\xi \in Q_p$，若 $ord_p(1 \pm \xi) > 1/(p-1)$，则 $ord_p(\log_p(\xi)) = ord_p(1 \pm \xi)$. 在应用中，我们将其用于

$$\xi = \alpha_0 \cdot \prod_{i=1}^{n} \alpha_i^{x_i}.$$

其中 $ord_p(\xi - 1)$ 是大的，这蕴涵着 $ord_p(\log_p(\xi))$ 也是大的．这里，我们是基于逼近格的定义．然而其逆未必成立：$ord_p(\log_p(\xi))$ 大不蕴涵 $ord_p(\xi - 1)$ 也大．这是由于 p－adic 对数是多维分支函数的缘故．更精确地，对任一个单位根 $\zeta \in Q_p$，有 $\log_p(\zeta) = 0$（参阅 2·3 节），若 p 是奇数，在 Q_p 中仅存在着第 (p－1) 个单位根，当 p＝2 时，仅有单位根 ±1．当 p 是奇数时，设 ξ 是第 (p－1) 个初始单位根，当 p＝2 时，设 ζ＝－1．由此，$ord_p(\log(\xi))$ 是大的蕴涵着对某个 $k \in \{0, 1, \cdots, p-2\}$（或 $k \in \{0, 1\}$，当 p＝2 时），有

$$\mathrm{ord}_p(\log_p(\xi)) = \mathrm{ordp}(\xi - \xi^k)$$

集合 $x_1, \cdots, x_n$ 使得 $\mathrm{ord}_p(\xi - 1)$(或 $\mathrm{ord}_p(\xi \pm 1)$, 若需要时)是大的. 结果是 Γ_μ 的子格 Γ_μ^*(或 $\Gamma_\mu^{非}$, 分别地). 在下面的引理, 我们将证明这一事实, 并指出怎样找到这子格的基. 然后, 我们可以用这一子格代替 Γ_μ 本身. 当然, 在引理 3·12, 3·14 和 3·16, 我们可用这子格 Γ_μ^*, $\Gamma_\mu^{非}$ 代替 Γ_μ. 为简单起见, 我们假定对所有 $i, \alpha_i \in Q_p$. 我们取 $\alpha_0 = 1$(因此对于齐次情形, 对应于 $\beta = 0$), 对 $\alpha_0 \neq 1$(非齐次情形), 我们把定义适当的变换格 $\Gamma_\mu^*(y)$, $\Gamma_\mu^{非}(y)$ 留给读者.

引理 3·17 (i) 设 $\alpha_1, \cdots, \alpha_n \in Q_p$ 是满足对所有 i, $\mathrm{ord}_p(\alpha_i) = 0$ 的给定的数, 且对 $i = n$, $\mathrm{ord}_p(\log_p(\alpha_i))$ 极小. 设 $x_1, \cdots x_n \in Z$, 令

$$\xi = \prod_{i=1}^{n} \alpha_i^{x_i}, \qquad \mu_0 = \mathrm{ord}_p(\log_p(\alpha_n)).$$

对任意 $\mu \in N_0$, 令

$$\Gamma_\mu = \{(x_1, \cdots x_n\} \in Z^n \mid \mathrm{ord}_p(\log_p(\xi)) \geqslant \mu + \mu_0\},$$

$$\Gamma_\mu^* = \{(x_1, \cdots, x_n) \in Z^n \mid \mathrm{ord}_p(\xi \pm 1) \geqslant \mu + \mu_0\},$$

$$\Gamma_\mu^{非} = \{(x_1, \cdots, x_n) \in Z^n \mid \mathrm{ord}_p(\xi - 1) \geqslant \mu + \mu_0\}.$$

则 $\Gamma_\mu^{非} \subseteq \Gamma_\mu^* \subseteq \Gamma_\mu$ 是格. 若 $p = 2$, 则它们都相等, 若 $p = 3$, 则 $\Gamma_\mu^* = \Gamma_\mu$. 若 $p \geqslant 3$, 则$_{非}(\Gamma_\mu / \Gamma_\mu^*) = (p-1)/2$, $_{非}(\Gamma_\mu / \Gamma_\mu^{非}) = p - 1$, $_{非}$

$(\Gamma_\mu^* / \Gamma_\mu^{\#}) = 2$.

(ii) 设 $\underline{b}_1, \cdots, \underline{b}_n$ 是 Γ_μ 的基, 对任意 $x \in [x_1, \cdots, x_n]^t \in \Gamma_\mu$, 用

$$\xi \equiv \zeta^{k(\underline{x})} \pmod{p^{\mu+\mu_0}}, \ k(\underline{x}) \in \{0, 1, \cdots, p-2\}.$$

定义 $k(\underline{x})$. 设 $\underline{b}'_1, \cdots, \underline{b}'_n$ 是 Γ_μ 的基, 使得

$$k(\underline{b}'_n) = \gcd[k(\underline{b}_1), \cdots, k(\underline{b}_n)]$$

对 $i = 1, \cdots, n-1$ 及 $p \geqslant 5$, 令

$$r_i^* \equiv k(\underline{b}_i')/k(\underline{b}_n') \pmod{(p-1)/2}, \ |r_i^*| \leqslant (p-1)/4,$$

$$\underline{b}_i^* = \underline{b}_i' - r_i^* \cdot \underline{b}_n'.$$

对 $p \geqslant 3$, 也有

$$r_i^{\#} \equiv k(\underline{b}_i')/k(\underline{b}_n') \pmod{(p-1)}, \ |r_i^{\#}| \leqslant (p-1)/2,$$

$$\underline{b}_i^{\#} = \underline{b}_i' - r_i^{\#} \cdot \underline{b}_n'.$$

进而, 对 $p \geqslant 5$, 令

$$r_n^* = \mathrm{lcm}[k(\underline{b}_n'), (p-1)/2]/k(\underline{b}_n'), \ \underline{b}_n^* = r_n^* \cdot \underline{b}_n'.$$

对 $p \geqslant 3$, 也令

$$r_n^{\#} = \mathrm{lcm}[k(\underline{b}_n'), (p-1)]/k(\underline{b}_n'), \ \underline{b}_n^{\#} = r_n^{\#} \cdot \underline{b}_n'.$$

则 $\underline{b}_1^*, \cdots, \underline{b}_n^*$ 是 Γ_μ^* 的基, $\underline{b}_1^{\#}, \cdots, \underline{b}_n^{\#}$ 是 $\Gamma_\mu^{\#}$ 的基.

证明 (i) $\Gamma_\mu^{\#} \subseteq \Gamma_\mu^* \subseteq \Gamma_\mu$ 是平凡的, 他们是格. 由 ± 1 是 $p = 2, 3$ 时 Q_p 中仅有的单位根导出 $p = 2, 3$ 时的格等式 $\#(\Gamma_\mu/$

Γ_μ^*)等等的值由(ii)导出.

(ii) 注意到 $k(\underline{x})$ 是(mod(p−1))Γ_μ 上的线性函数. Γ_μ^* 的点 x 具有 $(p-1)/|k(\underline{x})$ 的特征, $\Gamma_\mu^{非}$ 的点 x 具有 $(p-1)|k(x)$ 的特征. 由引理中的规定导出对 $i=1,\cdots,n-1$, 有

$$k(\underline{b}_i^*)\equiv k(\underline{b}_i')-r_i^*\cdot k(\underline{b}_n')\equiv 0 \quad (\bmod (p-1)/2),$$

$$k(\underline{b}_i^{非})\equiv k(\underline{b}_i')-r_i^{非}\cdot k(\underline{b}_n')\equiv 0 \quad (\bmod (p-1)).$$

注意到 $\underline{b}_1^*,\cdots\underline{b}_{n-1}^*,\underline{b}_n'$ 和 $\underline{b}_1^{非},\cdots,\underline{b}_{n-1}^{非},\underline{b}_n'$ 是 Γ_μ 的两个基(对整数 $y_i^*,y_i^{非}$), 写出 $\underline{x}\in\Gamma$ 如

$$\underline{x}=\sum_{i=1}^{n-1}y_i^*\cdot\underline{b}_i^*+y_n^*\cdot\underline{b}_n'=\sum_{i=1}^{n-1}y_i^{非}\cdot\underline{b}_i^{非}+y_n^{非}\cdot\underline{b}_n',$$

则导出

$$k(x)\equiv y_n^*\cdot k(\underline{b}_n') \ (\bmod (p-1)/2).$$

$$k(\underline{x})\equiv y_n^{非}\cdot k(\underline{b}_n') \ (\bmod (p-1)).$$

因此 $\underline{x}\in\Gamma_\mu^*$ 当且仅当 $r_n^*|y_n^*$, 而 $\underline{x}\in\Gamma_\mu^{非}$ 当且仅当 $r_n^{非}|y_n^{非}$. 这就证得结论.

第四章　双递归序列的 S－整数

4·1　导言

本章就下面的问题介绍一种简化解法．设 A, B, G_0, G_1 是整数，并设递归序列 $\{G_n\}_{n=0}^{\infty}$ 由

$$G_{n+1} = A \cdot G_n - B \cdot G_{n-1}, \quad n = 1, 2, \cdots$$

定义．假定 $\Delta = A^2 - 4 \cdot B$ 为非平方数，且序列为非退化的（这一点将在后面解释）．设 w 是非零整数，$p_1, \cdots p_s$ 是不同素数．我们研究丢番图方程

$$G_n = w \cdot \prod_{i=1}^{s} p_i^{m_i}, \tag{4·1}$$

其中 $n, m_1, \cdots, m_s$ 是非负整数．我们将研究判别式 Δ 为正的或为负的两种情形（双曲线型或椭圆型的情形）．Mahler[74]已证明(4·1)仅有有限多个解．对于 $\Delta > 0$ 的情形，Schinzel[101]已给出解的有效的可计算的上界．

Mignotte[78]，[79]指出(4·1)满足 $s = 1$ 的某些例子可用同余方法求解．但他的方法能否适合 $s = 1$ 时的任意方程(4·1)是不明确的．此外，他的方法似乎不能推广到 $s > 1$ 的情形．Pethö[91]基于 Gelfond－Baker 方法给出一种简化解法来处理(4·1)在 $\Delta > 0, w = s = 1$ 的情形．

我们的简化计算建立在 p－adic 丢番图逼近的简单情

形，即零维的情形，参阅 3·0 节．于双曲线型的情形，这已能满足找出方程(4·1)全部解的需要．在这种情形，是基于对 $|G_n|$ 指数增长的平常观察．在椭圆型的情形，情况本质上更难解．则从复的 Gelfond－Baker 理论可得到 $|G_n|$ 增长方面的资料．因此在此情形，我们有 p－adic 模拟与一维齐次或非齐次实丢番图逼近方法的结合，参考 3·2 和 3·3 节．

若方程的参数不太大，我们将给出(4·1)的解的小得容许简化计算实际应用的明确上界．Petho[91]指出，本质上更大的上界适用于所有的但也许是一种解．他的理由本质上与我们的简化技术相同．

一般的 Ramanujan－Nagell 方程

$$x^2 + k = \prod_{i=1}^{s} p_i^{z_i}, \tag{3·2}$$

其中 $k \in Z$ 固定，$x, z_1, \cdots, z_s \in N_0$ 是未知数，可以简化成有限多个满足 $\Delta > 0$ 的(4·1)类型的方程．满足 $s = 1$ 的方程(4·2)已有很长的历史(参阅 Hasse[54]，Cohen[34]，Ramasamy[99]等人的综述．关于此类方程解数方面的最好结果是由乐茂华[63，64，65]得到的．有趣的是应用于编码理论(参阅 Bremner，Calderbank，Hanlon，Morton 和 Wolfskill[22]，Macwilliams 和 Sloane[72]，Tzanakis 和 Wolfskill[126]，[127]，郭永东[50])．(4·2)的例子已由 Hunt 和 Van der Poorten 运用 Gelfond－Baker 理论解决．他们运用实的或复的但不是 p－adic 的对数线性型，正如我们熟知，没有人提出(4·2)的处理方法产生对 k 和 p_i 的任意值起作用的计算，而 Tzanakis 的初等方法(参见 Tzanakis[121])似乎是能推广到 $s > 1$ 的唯一方法．

我们的方法有两者的性质.

本章的组织如下.4·2 节给出一些初步的双递归序列.4·3 节就双曲线型和椭圆型两情形研究 $|G_n|$ 的增长.双曲线型的情况是平凡的.在椭圆型的情形,我们通过证明关于 n 的依赖于 v 的特别良好的一个上界,并说明如何降低这个界,给出对固定的 $v \in R$ 解 $|G_n| < v$ 的一种方法.4·4 节给出(4·1)解的上界.4·5 节给出一个引理,其中简化程序的 p-adic 部分是基本的.4·6 节处理一些特别情形,计算'对称'递归.对于递归序列的特殊类型,我们的简化计算失效,但在此情形,初等幅角常用于解(4·1).4·7 就一些精心挑选的例子,给出降低方程(4·1)在 $\Delta > 0$ 时解的上界的运算.4·8 节中关于 $\Delta < 0$ 的情形做法相同.4·9 节阐明怎样处理一般的 Ramanujan-Nagell 方程,这作为(4·1)的双曲线型的一种应用.作为一个例子,我们确定所有整数 x 使得 $x^2 + 7$ 没有比 20 更大的素因子,因此扩充了 Nagell[86]关于方程 $x^2 + 7 = 2^n$(最初的 Ramanujan-Nagell 方程)的结果.最后,在 4·10 节,我们给出(4·1)的椭圆型情形在一定类型的带平方指数丢番图方程的一种应用,这类似于解(4·2)的双曲线型情形的应用.作为例子,我们可以确定方程

$$x^2 - 3^{m_1} \cdot 7^{m_2} \cdot x + 2 \cdot [3^{m_1} \cdot 7^{m_2}]^2 = 11 \cdot 2^n$$

的解 x, m_1, m_2, n.

4·2 双递归序列

设 $A, B, G_0, G_1 \in Z$ 给定.设序列 $\{G_n\}_{n=0}^{\infty}$ 由

$$G_{n+1}=A\cdot G_n-B\cdot G_{n-1},\ n=1,2,\cdots \tag{4·3}$$

定义. 设 α,β 是 $x^2-Ax+B=0$ 的根. 假定 $\Delta=A^2-4\cdot B$ 是非平方数, 且 α/β 不是单位根(即序列是非退化的). 令

$$\lambda=\frac{G_1-G_0\cdot\beta}{\alpha-\beta},\ \mu=\frac{G_0\cdot\alpha-G_1}{\alpha-\beta} \tag{4·4}$$

则 λ 和 μ 在 $K=Q(\sqrt{\Delta})$ 中是共轭的. 对所有 n, 现在有

$$G_n=\lambda\cdot\alpha^n+\mu\cdot\beta^n \tag{4·5}$$

(参看 Shorey 和 Tijdeman[107], 定理 C. 1). 我们将表明, 当解(4·1)时, 不失一般性, 可假定

$$(G_0,G_1)=(G_1,B)=(A,B)=1.$$

即: 若 $d=(G_0,G_1)$, 则 $d\mid G_n$(对所有 $n\geqslant 0$), 因此我们研究(4·1)可用 $G_n'=G_n/d$ 代替 G_n. 其次假定 $d=(A,B)$. 若也有 d^2 B, 则容易验证对所有 $n\geqslant 2$, 有 d^{n-1} G_n. 则我们考虑(4·1)用 $G_n'=G_{n+1}/d^n$ 代替 G_n. 使得 $G_{n+1}'=A'\cdot G_n'-B'G'_{n-1}$ 的 A', B' 是 $A'=A/d$, $B'=B'/d^2$, 因此 $(A',B')=1$. 然而, 若 $d^2\nmid B$, 则我们将序列分离成两部分. 我们考虑(4·1)首先用 $G'=G_{2\cdot n}$ 代替 G_n, 然后用 $G_n'=G_{2\cdot n+1}$ 代替 G_n. 对于两个序列 $\{G_n'\}$, 使得 $G_{n+1}'=A'\cdot G_n'-B'\cdot G_{n-1}'$ 的 A', B' 由 $A'=A^2-2\cdot B$, $B'=B^2$ 给出. 则 $(A',B')=d$ 且 d^2 B', 因此我们回到先前的情形. 最后, 设 p 是一个素数使得 $p\mid(G_1,B)$, 并设 $\mathfrak{p}$ 是 $Q(\sqrt{\Delta})$ 落在 p 上的素理想. 由 $p\mid B=\alpha\cdot\beta$, 有 $\mathfrak{p}$ (α) 或 $\mathfrak{p}\mid(\beta)$. 假定 $\mathfrak{p}\mid(\alpha)$, 则 $\mathfrak{p}\nmid(\beta)$, 因 $(A,B)=1$(注意 $A=\alpha+\beta$). 因此,

$$\mathrm{ord}_p(\lambda\cdot\alpha^n+\mu\cdot\beta^n)=\min[\mathrm{ord}_p(\lambda\cdot\alpha^n),\mathrm{ord}_p(\mu\cdot\beta^n)]=\mathrm{ord}_p(\mu)$$

若对某 n_0, $n\geqslant n_0$. 因此对 $n\geqslant n_0$, $\mathrm{ord}_p(G_n)$是常数. 若 $p|(\beta)$, 同样正确. 故我们可假定$(G_1,B)=1$.

引理 4·1　设 $n, m_1, \cdots m_s$ 是(4·1)的解, 则满足上述假定, 对 $i=1,\cdots,s$, 或者 $m_i=0$ 或者 $n=0$ 或者

$$\begin{aligned}&\mathrm{ord}_{p_i}(\alpha)=\mathrm{ord}_{p_i}(\beta)=0\\&\mathrm{ord}_{p_i}(\lambda)=\mathrm{ord}_{p_i}(\mu)=-\frac{1}{2}\cdot\mathrm{ord}_{p_i}(\Delta)\leqslant 0\end{aligned}\tag{4·6}$$

证明　假设 $p_i|B$. 则 $p_i\nmid A$ 因此由(4·3)和$(B,G_1)=1$, 对所有 $n\geqslant 1$, 有 $p_i\nmid G_n$. 因此, $m_i=0$ 或 $n=0$. 其次假设 $p_i\nmid B$, 则由 $\alpha\cdot\beta=B$.

$$\mathrm{ord}_{p_i}(\alpha)+\mathrm{ord}_{p_i}(\beta)=\mathrm{ord}_{p_i}(B)=0.$$

现在, α 和 β 是代数整数. 因此, 他们的 p - adic 次数是非负的. 这就导出他们是零. 令 $E=-\lambda\cdot\mu\cdot\Delta$, 注意 $E\in Z$, 且对所有 $n\geqslant 0$,

$$G_{n+1}^2-A\cdot G_n\cdot G_{n+1}+B\cdot G_n^2=E\cdot B^n.$$

假定 $p_i|E$, 则推出对所有 n, $p_i\nmid G_n$, 因为$(G_0,G_1)=1$. 因此 $m_i=0$. 其次假定 $p_i\nmid E$, 则

$$\mathrm{ord}_{p_i}(\lambda\cdot\sqrt{\Delta})+\mathrm{ord}_{p_i}(\mu\cdot\sqrt{\Delta})=\mathrm{ord}_{p_i}(E)=0.$$

因为 $\lambda\cdot\sqrt{\Delta}$和 $\mu\sqrt{\Delta}$是代数整数(注意$\sqrt{\Delta}=\alpha-\beta$), 便得结论.

由引理 2·1 导出, 我们可不失一般性地假定(4·6)对 $i=1,\cdots,s$ 成立. 也可假定对 $i=1,\cdots,s$, $\mathrm{ord}_{p_i}(w)=0$. 方程(4·1)

中 $s=0$ 的特别情形当 $\Delta>0$ 时是平凡的，而对所有 Δ，将包含在下一节中处理.

4·3 递归序列的增长

首先我们处理双曲线型情形 $\Delta>0$. 注意到 $|\alpha|\neq|\beta|$，因为序列不是退化的. 因此可假定 $|\alpha|>|\beta|$. 我们导出，序列 $\{G_n\}_{n=0}^{\infty}$ 指数增长结果几乎是平凡的. 设

$$n_0>\max[2,\log|\frac{\mu}{\lambda}|/\log|\frac{\alpha}{\beta}|],$$

$$r=|\lambda|-|\mu|\cdot|\frac{\alpha}{\beta}|^{-n_0}.$$

注意 $r>0$.

引理 4·2　设 $\Delta>0$. 若 $n\geqslant n_0$，则 $|G_n|\geqslant r\cdot|\alpha|^n$.

证明　由(4·5)，$|\alpha|>|\beta|$ 且 $n_0>0$ 导出，对 $n\geqslant n_0$，

$$|G_n|\cdot|\alpha|^{-n}=|\lambda+\mu\cdot[\frac{\alpha}{\beta}]^{-n}|\geqslant|\lambda|-|\mu|\cdot|\frac{\alpha}{\beta}|^{-n}\geqslant r.$$

我们将其应用于(4·1)如下.

推论 4·3　设 $\Delta>0$. (4·1)在 $n\geqslant n_0$ 时的任意解 $n, m_1, \cdots, m_s$ 满足

$$n<\sum_{i=1}^{s}m_i\cdot\frac{\log p_i}{\log|\alpha|}-\frac{\log(r/|w|)}{\log|\alpha|}.$$

证明　显然，由引理 4·2 及(4·1)即得.

下面研究椭圆型情形 $\Delta<0$. 因为 α/β 不是单位根，故 $B\geqslant 2$. 因为 (α,β) 及 (λ,μ) 是成对的复共轭，故 $|\alpha|=|\beta|$，$|\lambda|=|\mu$

令 $v\in R, v\geq 1$ 给定. 我们研究不等式

$$|G_n|\leq v \qquad (4\cdot 7)$$

其中 $n\in N$ 是变量. 我们应用来自超越数论对数线性型的 Waldshmit 的一个结果(见 2·3 节), 它给出用 C_3 表示的特别良好的关于 n 的一个上界. 也可参看 Kiss[55]. 设

$$E=-\lambda\cdot\mu\cdot\Delta,$$

$$V_2=\frac{1}{2}\cdot\max(\pi,\log B),\quad V_3=\frac{1}{2}\max(\pi,\log E),$$

$$V_2^+=\min(V_2,V_3),\quad V_3^+=\max(V_2,V_3),$$

$$C_1=3.362\times 10^{21}\cdot V_2\cdot V_3\cdot\log(2\cdot e\cdot V_2^+),$$

$$C_2=\log(4\cdot e\cdot V_3^+),$$

$$C_3=\max[\log(\pi/2\cdot|\mu|)+C_1\cdot C_2+C_1\cdot\log(4\cdot C_1/\log B),$$

$$\frac{1}{2}\cdot\log|\lambda\cdot\sqrt{\Delta}|]\cdot 4/\log B$$

定理 4·4 设 $\Delta<0, v\in R, v\geq 1$. 若 $n\geq 0$ 满足(4·7), 则

$$n<C_3+\frac{4}{\log B}\cdot\log v.$$

注: 注意 C_3 不依赖于 v.

定理 4·4 直接导出下面推论.

推论 4·5 设 $\Delta<0$, (4·1)的任意解 $n, m_1, \cdots, m_s$ 满足

$$n < C_3 + \frac{4}{\log B}\cdot\left(\log|w| + \sum_{i=1}^{s} m_i\cdot\log p_i\right).$$

定理 4·4 的证明　注意 $|\alpha| = |\beta| = \sqrt{B} \geqslant \sqrt{2}$. 首先我们处理 $G_n = 0$ 的情形. Kiss[55]给出了这样的 n 的一个上界,但由于在我们的条件 $(G_0, G_1) = (G_1, B) = (A, B) = 1$ 之下,我们可做得更好. 即:令 $R_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ 对所有 $n \in Z$ 成立. 容易看出,$R_n \in Z$ 且 $R_{-n} = -B^{-n}\cdot R^n$ 对所有 $n \in Z$ 成立. 现在 $G_{n_0} = \lambda\cdot\alpha^{n_0} + \mu\beta^{n_0} = 0$ 蕴含

$$\begin{aligned} G_n &= \lambda\cdot\alpha^{n_0}\cdot\alpha^{n-n_0} + \mu\cdot\beta^{n_0}\cdot\beta^{n-n_0} \\ &= \lambda\cdot\alpha^{n_0}\cdot\sqrt{\Delta}\cdot R_{n-n_0} \\ &= -\lambda\cdot\beta^{-n_0}\cdot\sqrt{\Delta}\cdot B^n\cdot R_{n_0-n}. \end{aligned}$$

因此有

$$G_0 = [-\lambda\cdot\beta^{-n_0}\cdot\sqrt{\Delta}]\cdot R_{n0},$$

$$G_1 = [-\lambda\cdot\beta^{-n_0}\cdot\sqrt{\Delta}]\cdot B\cdot R_{n_0-1}$$

假定对于 $Q(\sqrt{\Delta})$ 中的某素理想 $\wp$, 有 $\wp|(R_n, B\cdot R_{n-1})$. 则 $\wp|(\alpha\cdot R_n - B\cdot R_{n-1}) = (\alpha)^n$, 且 $\wp|(\beta R_n - B\cdot R_{n-1} = (\beta)^n$, 这与 $(A, B) = 1$ 矛盾. 因此 $(R_n, B\cdot R_{n-1}) = 1$, 则由 $(G_0, G_1) = 1$, 必有

$$|\lambda\cdot\beta^{-n_0}\cdot\sqrt{\Delta}| = 1.$$

因此我们发现 $G_n = 0$ 蕴含

$$n = \frac{2}{\log B} \cdot \log|\lambda \cdot \sqrt{\bar{\Delta}}| < C_3.$$

现在回到 $G_n \neq 0$ 的情形. 由(4·7)有

$$\left| [\frac{-\lambda}{\mu}] \cdot [\frac{\alpha}{\beta}]^n - 1 \right| \leqslant \frac{v}{|\mu|} \cdot B^{-n/2}.$$

我们可假定 $n \geqslant 2$. 设 $-\lambda/\mu = e^{2\pi i \cdot \psi}$, $\alpha/\beta = e^{2\pi i \cdot \varphi}$ 满足 $-\frac{1}{2} < \psi \leqslant \frac{1}{2}$ 及 $-\frac{1}{2} < \varphi \leqslant \frac{1}{2}$. 设 $K \in Z$ 使得 $|\psi + n \cdot \varphi + K| \leqslant \frac{1}{2}$. 则 $|K| \leqslant 1 + \frac{1}{2} \cdot n \leqslant n$. 令

$$\begin{aligned} \Lambda &= 2\pi i \cdot [\psi + n \cdot \varphi + K] \\ &= \log[\frac{-\lambda}{\mu}] + n \cdot \log[\frac{\alpha}{\beta}] + 2 \cdot K \cdot \log(-1). \end{aligned}$$

由引理 2·3 和(4·8)我们得到 $|\Lambda|$ 的一个上界:

$$\begin{aligned} |\Lambda| &= 2\pi \cdot |\psi + n \cdot \varphi + K| \leqslant \frac{1}{2}\pi \cdot |e^{2\pi i \cdot (\psi + n \cdot \varphi + K)} - 1| \\ &= \frac{1}{2}\pi \cdot |[\frac{-\lambda}{\mu}] \cdot [\frac{\alpha}{\beta}]^n - 1| \leqslant \frac{1}{2}\pi \cdot \frac{v}{|\mu|} \cdot B^{-n/2}. \end{aligned} \quad (4 \cdot 9)$$

由 $G_n \neq 0$ 导出 $\Lambda \neq 0$. 则由引理 2·4 我们可导出 $|\Lambda|$ 的一个下界. 注意到 $\max(n, 2|K|) \leqslant 2 \cdot n$, 所以 $w = \log(2 \cdot n)$. 我们选择 $v_1 = \frac{1}{2}$. 数 $z = \alpha/\beta$ 满足

$$B\cdot z^2-(A^2-2\cdot B)\cdot z+B=0,$$

因此 $h(\alpha/\beta)\leqslant\frac{1}{2}\cdot\log B$. 又 $z=-\lambda/\mu$ 满足

$$E\cdot z^2-(2\cdot E+\Delta\cdot G_0^2)\cdot z+E=0,$$

因此 $h(-\lambda/\mu)\leqslant\frac{1}{2}\cdot\log E$. 因此 $v_2=V_2^+$, $v_3=V_3^+$ 满足要求.
由定理 2·4, 我们发现

$$|\Lambda|>\exp[-C_1\cdot(\log(2\cdot n)+\log(2\cdot e\cdot V_3^+))]$$
$$=\exp[-C_1\cdot(\log n+C_2)]. \tag{4·10}$$

结合(4·9)和(4·10)我们找到 $n<a+b\cdot\log n$, 其中

$$a=\frac{2}{\log B}\cdot[\log v+\log\frac{\pi}{2\cdot|\mu|}+C_1\cdot C_2],$$

$$b=2\cdot C_1/\log B.$$

由引理 2·1 可导出结论, 因为

$$b=2\cdot C_1/\log B$$
$$=1.681\times10^{21}\cdot\frac{\max(\pi,\log B)}{\log B}\cdot\max(\pi,\log E)\cdot\log(2\cdot e\cdot V_2^+)$$

这必定比 e^2 大.

注释: 注意 v 可依赖于 n, 因此我们可找到关于解 $n\in N_0$ 的一个上界, 例如对常数 c, 有 $|G_n|\leqslant n^c$.

现在, 我们想降低定理 4·3 中找到的界. 为此, 研究丢番

图不等式

$$|\psi + n\cdot\varphi + K| < v_0 \cdot B^{-n/2}. \qquad (4\cdot 11)$$

此不等式由(4·9)导出，其中 $v_0 = v/4\cdot|\mu|$. 我们已区别齐次情形 $\psi=0$ 及非齐次情形 $\psi\neq 0$. 分别运用在3·2节及3·3节中叙述的方法. 不象其他章，这里我们用精确规定的运算方式给出结果.

首先研究齐次情形 $\psi=0$. 我们采用运算H(见图表4). 设N是(4·11)的解n的上界，例如定理4·3中找到的界.

图表4. 运算H(降低(4·11)在 $\psi=0$ 时的上界)

Input: $\varphi, B, |\mu|, v_0, N$

Output: new, reduced bound N' for n.

(i) (initialization) Choose $n_0 \geqslant 2/\log B$ such that $B^{n_0/2}/n_0 \geqslant 2\cdot v_0$;

$N_0 := N$; compute the continued fraction

$$|\varphi| = [0, a_1, a_2, \cdots, a_{t_0+1}, \cdots]$$

and the denominators $q_1, \cdots, q_{t_0+1}$ of the convergents of $|\varphi|$, wich t_0 so large that $q_{t_0} \leqslant N_0 < q_{t_0+1}$; $i := 0$;

(ii) (compute new bound) $A_i := \max(a_1, \cdots, a_{t_i+1})$; compute the largest integer N_{i+1} such that

$$B^{N_{i+1}/2}/N_{i+1} \leqslant v_0\cdot(A_i+2),$$

and t_{i+1} such that $q_{t_{i+1}} \leqslant N_{i+1} < q_{t_{i+1}+1}$;

(iii) (terminate loop)

if $n_0 \leqslant N_{i+1} < N_i$ then $i := i+1$, goto (ii);

else $N' := \max(n_0, N_{i+1})$, stop.

引理 4·6　运算 H 结束. 不等式(4·11)在 $\psi=0$ 时没有满足 $N^*<n<N$ 的解.

证明　结果是显然的, 因为所有 N_i 是整数. 注意 $B^{x/2}/x$ 在 $x>2/\log B$ 时是递增函数. 因此, 若 $n\geqslant n_0$, 则

$$\left| |\varphi| - |k|/n \right| \leqslant v_0 \cdot B^{-n/2}/n < 1/2n^2.$$

由此推出(见(3·6)) $|\varphi|$ 收敛于 $|k|/n$, 比如 $|k|/n = P_m/q_m$. 则 $q_m\leqslant n$, 且(见(3·5))

$$\left| |\varphi| - P_m/q_m \right| > 1/(a_{m+1}+2)\cdot q_m^2.$$

假定对某个 $i\geqslant 0$, $n\leqslant N_i$, 则 $m<c_i$, 因此

$$\begin{aligned} B^{n/2}/n &\leqslant v_0\cdot n^{-2}\cdot \left| |\varphi| - |k|/n \right|^{-1} < v_0\cdot(a_{m+1}+2) \\ &\leqslant v_0\cdot(A_m+2). \end{aligned}$$

由此得到, 若 $N_{i+1}\geqslant n_0$, 则 $n\leqslant N_{i+1}$.

其次研究非齐次情形 $\psi\neq 0$. 再设 N 是满足(4·11)的 n 的一个上界. 我们有下面运算 I(见图表 5.)

图表 5. 运算 I. (降低(4·11)在 $\psi\neq 0$ 时的上界)

Input: φ, ψ, B, v_0, N.

Output: new, reduced upper bound N^* for all but a finite number of explicitly given

n.

(i) (initialization $N_0 := [N]$; compute the continued fraction

$$|\varphi| = [0, a_1, a_2, \cdots, a_{t_0}, \cdots]$$

and the convergents p_i/q_i for $i = 1, \cdots, t_0$, with t_0 so large that $q_{t_0} > 4 \cdot N_0$ and $\| q_{t_0} \cdot \psi \| > 2 \cdot N_0 / q_{t_0}$. (If such t_0 cannot be found within reasonable time, take t_0 so large that $q_{t_0} > 4 \cdot N_0$); $i := 0$;

(ii) (compute new bound)

<u>if</u> $\| q_{t_0} \cdot \psi \| > 2 \cdot N_i / q_{t_i}$

<u>then</u> $N_{i+1} := [2 \cdot \log(q_{t_i}^2 \cdot v_0 / N_i) / \log B]$;

else compute $K \in Z$ with $|K - q_{t_i} \cdot \psi| \leqslant \frac{1}{2}$; compute $n_0 \in Z, 0 \leqslant n_0 < q_{t_i}$, with $K = n_0 \cdot p_{t_i} = 0 (\mathrm{mod}\, q_{t_i})$; <u>if</u> $n = n_0$ is a solution of (4.11),

<u>then</u> print an appropriate message;

$N_{i+1} := [2 \cdot \log(4 \cdot q_{t_i} \cdot v_0) / \log B]$;

(iii) (terminate loop)

<u>if</u> $N_{i+1} < N_i$

<u>then</u> $i := i + 1$; compute the minimal $t_i < t_{i-1}$ such that $q_{t_i} > 4 \cdot N_i$ and $\| q_{t_i} \cdot \psi \| > 2 \cdot N_i / q_{t_i}$ (if such t_i does not exist, choose the minimal t_i wich $q_{t_i} > 4 \cdot N_i$); <u>goto</u> (ii);

<u>else</u> $N^* := N_i$; <u>stop</u>.

引理 4·7 运算 I 终止. 不等式(4·11)在 $\psi \neq 0$ 时, 由运算找出 $N^* < n < N$ 仅有有限多个解.

证明 运算终止是显然的. 假定对某 $i \geqslant 0$, $n \leqslant N_i$, 则当 $\| q_{t_i} \cdot \psi \| > 2 \cdot N_i / q_{t_i}$ 时, 有

$$\| q_{t_i} \cdot \psi \| = \| q_{t_i} \cdot (\psi + n \cdot \varphi + k) - n \cdot \varphi \cdot q_{t_i} \|$$

$$\leqslant q_{t_i} \cdot |\psi + n \cdot \varphi + k| + n / q_{t_i} \leqslant q_{t_i} \cdot v_0 \cdot B^{-n/2} + N_i / q_{t_i}.$$

由此推出 $n \leqslant N_{i+1}$. 若 $\| q_{c_i} \cdot \psi \| \leqslant 2 \cdot N_i / q_{c_i}$, 因此

$$|k + n \cdot p_{c_i} + k \cdot q_{c_i}| \leqslant |k - q_{c_i} \cdot \psi| + q_{c_i} \cdot |\psi + n \cdot \varphi + k| + n \cdot |p_{c_i} - q_{c_i} \cdot \varphi|$$

$$\leqslant \frac{1}{2} + q_{c_i} \cdot v_0 \cdot B^{-n/2} + N_i / q_{c_i} < \frac{3}{4} + q_{c_i} \cdot v_0 \cdot B^{-n/2}.$$

若 $q_{c_i} \cdot v_0 \cdot B^{-n/2} \leqslant \frac{1}{4}$, 则 $K + n \cdot p_{c_i} + K \cdot q_{c_i} = 0$, 这是因为它是一个整数. 由 $(p_{c_i}, q_{c_i}) = 1$ 导出 $n \equiv n_0 (\bmod q_{c_i})$. 因 $q_{c_i} > N_i$, 仅能是 $n = n_0$. 若 $q_{c_i} \cdot v_0 \cdot B^{-n/2} > \frac{1}{4}$, 则 $n \leqslant N_{i+1}$ 导出矛盾.

我们注意到, 若 N_i 足够大, 则实际上几乎都可找到一个 c_i 使得 $\| q_{c_i} \cdot \psi \| > 2 \cdot N_i / q_i$.

4·4 上界

本节就双曲线型和椭圆型两情形, 我们要导出(4·1)解的显式上界. 第一步是 p－adic 理论的对数线性型之应用. 这对两种情形做法是相同的. 我们用其找出关于 m_i 的界是 logn 的多项式. 然后我们将其与 4·3 节中关于双递归序列增长方面的结果结合起来, 在那里我们对(4·1)的解导出关于 n 的界对 m_i 是线性的(推论 4·3 和 4·5).

假定 $n_0 \geqslant 2$. 设 D 是 $Q(\sqrt{\Delta})$ 的判别式. 令

$$L = \log\max[|e \cdot D|^{1/4}, |\alpha \cdot \lambda \cdot \sqrt{\Delta}|, |\alpha \cdot \mu \cdot \sqrt{\Delta}|, |\beta \cdot \lambda \cdot \sqrt{\Delta}|, |\beta \cdot \mu \cdot \sqrt{\Delta}|].$$

设 d 是 Δ 的无平方部分, 对 $i = 1, \cdots, s$, 令

$$\varphi_i = \begin{cases} 2, \text{当 } p_i | \text{ 时}; \\ 1, \text{其余情形}. \end{cases}$$

$$\rho_i = \begin{cases} 2, \text{若 } p_i = 2, d \equiv 5 (\mathrm{mod} 8) \text{ 或 } p_i > 2, \left(\frac{d}{p_i}\right) = -1; \\ 1, \text{其余情形}. \end{cases}$$

$$C_{4,i} = 10^6 \cdot \left[\frac{2}{\rho_i \cdot \log p_i}\right]^7 \cdot \varphi_i^{-3} \cdot L^4 \cdot p_i^{4 \cdot \rho_i + 4} \cdot \left[1 + \frac{\varphi_i \cdot L \cdot p_i^{\rho_i} + 2/L}{\log n_0}\right].$$

引理 4·8 $n \geqslant n_0$ 时(4·1)的解满足

$$m_i < C_{4,i} \cdot (\log n)^3, \quad i = 1, \cdots, s.$$

证明 利用(4·5)将(4·1)改写成

$$\left[\frac{\alpha}{\beta}\right]^n - \left[\frac{-\mu}{\lambda}\right] = \frac{w}{\lambda} \cdot \beta^{-n} \cdot \prod_{i=1}^{s} p_i^{m_i}.$$

则由(4·6),

$$m_i \leqslant m_i - \mathrm{ord}_{p_i}(\lambda) = \mathrm{ord}_{p_i}\left[\frac{w}{\lambda} \cdot \beta^{-n} \cdot \prod_{i=1}^{s} p_i^{m_i}\right] =$$

$$\mathrm{ord}_{p_i}\left[\left[\frac{\alpha}{\beta}\right] - \left[\frac{-\mu}{\lambda}\right]\right].$$

应用引理 2·5(Schinzel 的结果),当 $\xi'' = \alpha, \xi' = \beta, x'' = \mu \cdot \sqrt{\Delta}, x = -\lambda \cdot \sqrt{\Delta}$ 时,由 $\mathrm{ord}_{p_i}(\cdot) = \varphi_i \cdot \mathrm{ord}_{p_i}(\cdot)$,则得

$$m_i < 10^6 \cdot \left[\frac{2}{\rho_i \cdot \log p_i}\right]^7 \cdot \varphi_i^{-3} \cdot L^4 \cdot P_i^{4 \cdot \rho_i + 4}.$$

$$[\log n + \varphi_i \cdot L \cdot P_i^{\varphi_i} + 2/L]^3,$$

由于 $n \geqslant n_0$，便导出结论．

设

$$C_4 = \max_i(C_{4,i}),\ m = \max_i(m_i),\ p = \prod_{i=1}^{s} p_i.$$

在 $\Delta > 0$ 的情形，设 $n_0 > \max[2, \log|\lambda/\mu|/\log|\alpha/\beta|]$，并令

$$C_5 = \log P/[\log|\alpha| + \min(0, \log(r/|w|))],$$

$$C_6 = \max[8 \cdot C_4 \cdot (\log 27 \cdot C_4 \cdot C_5)^3, 841 \cdot C_4].$$

在 $\Delta < 0$ 的情形，令

$$C_7 = \max\left\{C_3 + \frac{4}{\log B} \cdot \log[2 \cdot |G_0 \cdot \mu\sqrt{\Delta}|],\right.$$
$$8 \cdot [[C_3 + \frac{4 \cdot \log|w|}{\log B}]^{1/3} + [\frac{4 \cdot C \cdot \log P}{\log B}]^{1/3} \cdot$$
$$\left.\log[\frac{108 \cdot C_4 \cdot \log P}{\log B}]]^3\right\},$$
$$C_{8,i} = C_{4,i} \cdot (\log C_7)^3,\ i = 1, \cdots, s.$$

则有下面给出(4·1)解的显式上界的结果．

定理 4·9　设 $n, m_1, \cdots, m_s$ 是(4·1)的解．

(i) 若 $\Delta > 0$ 且 $n \geqslant n_0$，则 $n < C_5 \cdot C_6$ 且 $m < C_6$．

(ii) 若 $\Delta < 0$，则 $n < C_7$，$m_i < C_{8,i}$，其中 $i = 1, \cdots, s$．

证明 (i) 推论 4·3 导出 $n<C_5\cdot m$. 由引理 4·8, 有

$$m<C_4\cdot(\log n)^3<C_4\cdot(\log C_5\cdot m)^3.$$

若 $C_4\cdot C_5>(e^2/3)^3$, 则对 $a=0, b=C_4\cdot C_5, h=3$ 应用引理 2·1, 我们有 $m<8\cdot C_4\cdot(\log 27\cdot C_4\cdot C_5)^3$. 若 $C_4\cdot C_5\leqslant(e^2/3)^3$, 则

$$n<C_5\cdot m<C_4\cdot C_5\cdot(\log n)^3\leqslant(e^2/3)^3\cdot(\log n)^3.$$

由此推出 $n<12564$. 现在, $m<C_4\cdot(\log n)^3<841\cdot C_4$.

(ii) 由引理 4·8 和推论 4·5 看出,

$$n<C_3+\frac{4}{\log B}\cdot\log[2\cdot|G_0\cdot\mu\cdot\sqrt{\Delta}|],$$

或

$$n<C_3+\frac{4\cdot\log|w|}{\log B}+\frac{4\cdot C_4\cdot\log P}{\log B}\cdot(\log n)^3.$$

由于 $4\cdot C_4\cdot\log P/\log B>(e^2/3)^3$, 故由引理 2·1 便得结论.

4·5 一个基本引理

我们引入一些记号, 然后给出一个似乎是平凡的引理, 它是对双曲线型和椭圆型两种情况的简化方法的中心. 对 $i=1,\cdots,s$, 设

$$e_i=-\mathrm{ord}_{p_i}(\lambda),\ f_i=\mathrm{ord}_{p_i}(\log_{p_i}[\alpha/\beta]),\ g_i=f_i-e_i$$

$$\theta_i=-\log_{p_i}\left[\frac{-\lambda}{\mu}\right]/\log_{p_i}\left[\frac{\alpha}{\beta}\right].$$

由引理 4·1, α/β 及 $-\lambda/\mu$ 的 p_i-adic 对数存在. 注意 $\log_{p_i}(\alpha/$

$\beta) \neq 0$，因为数列$\{G_n\}$是非退化的. 注意对于共轭数ξ, ξ'，$\log_p \xi$和$\log_p \xi'$也共轭，因此$\log_p(\xi/\xi') \in \sqrt{\Delta} \cdot Q_p$. 因此$\theta_i$的分子和分母都在$\sqrt{\Delta} \cdot Q_{p_i}$中，故$\theta_i \in Q_{p_i}$. 因此，若$\theta_i \neq 0$，我们可写出

$$\theta_i = \sum_{\iota = k_i}^{\infty} u_{i,\iota} \cdot p_i^{\iota}.$$

其中，对所有ι，$k_i = \mathrm{ord}_{p_i}(\theta_i)$，$u_{i,\iota} \in \{0, 1, \cdots, p_i - 1\}$. 下列引理使$\{G_n\}$的元素局部满足关于$\theta_i$的$p_i$ - adic 展式的许多因子p_i.

引理 4·10　设$n \in N_0$. 若$\mathrm{ord}_{p_i}(G_n) + e_i > 1/(p_i - 1)$，则

$$\mathrm{ord}_{p_i}(G_n) = g_i + \mathrm{ord}_{p_i}(n - \theta_i).$$

证明　由引理 4·1，有

$$\mathrm{ord}_{p_i}(G_n) + e_i = \mathrm{ord}_{p_i}\left[[\frac{\alpha}{\beta}]^n - [\frac{-\mu}{\lambda}] \right] = \mathrm{ord}_{p_i}\left[[\frac{-\lambda}{\mu}] \cdot [\frac{\alpha}{\beta}]^n - 1 \right].$$

由于$\xi = (-\lambda/\mu) \cdot (\alpha/\beta)^n - 1$，根据假定，我们有$\mathrm{ord}_{p_i}(\xi) > 1/(p_i - 1)$. 因此$\mathrm{ord}_{p_i}(\xi) = \mathrm{ord}_{p_i}(\log_{p_i}(1 + \xi))$. 由此导出

$$\mathrm{ord}_{p_i}(G_n) + e_i = \mathrm{ord}_{p_i}\left[n \cdot \log_{p_i}[\frac{\alpha}{\beta}] + \log_{p_i}[\frac{-\lambda}{\mu}] \right] = \mathrm{ord}_{p_i}(n - \theta_i) + f_i.$$

4·6 平凡的情形

我们首先排除一些平凡的情形.第一种平凡的情形是 $\mathrm{ord}_{p_i}(\theta_i)<0$.则(4·1)的解满足 $m_i\leqslant 1/(p_i-1)-e_i$,或由引理 4·10,

$$m_i=f_i-e_i+\mathrm{ord}_{p_i}(n-\theta_i).$$

由于 $n\in\mathbb{Z}$ 且 $\mathrm{ord}_{p_i}(\theta_i)<0$,故有 $\mathrm{ord}_{p_i}(n-\theta_i)=\mathrm{ord}_{p_i}(\theta_i)$,故

$$m_i\leqslant\max[f_i+\mathrm{ord}_{p_i}(\theta_i),1/(p_i-1)]-e_i.$$

θ_i 的所有 p_i - adic 数从某点起全为零是一种特别情形,因为下节的简化方法不能用.这是由于这种简化方法适用于零维 p - adic 丢番图逼近,如同 3·9 节所说明,应用于 p - adic 线性型

$$\log_p[\frac{\lambda}{\mu}]+n\cdot\log_p[\frac{\alpha}{\beta}],$$

其中 $p=p_1,\cdots,p_s$.这意味着我们必须研究 p - adic 数

$$\theta=-\log_p[\frac{\lambda}{\mu}]/\log_p[\frac{\alpha}{\beta}].$$

若发生这样的情形:这个数 θ 是零,或者 θ 的 p - adic 展式中的所有数字从某点起全为零,则显然地,3·9 的简化程序被破除,原因是基于根据假设,θ 的 p - adic 展式包含充分多的非零数字.

这一情形论及如下.注意对所有 $i=1,\cdots,s$ 及同一个 r,$\theta_i=r$ 成立.因此由引理 4·10,

$$m_i \leqslant \max[g_i + \mathrm{ord}_{p_i}(n-r), 1-e_i] \leqslant g_i + 1 + \mathrm{ord}_{p_i}(n-r). \quad (4\cdot 12)$$

若 $\Delta>0$，由推论 4·3，有

$$n\cdot \log|\alpha| < \sum_{i=1}^{s}(g_i+1)\cdot \log p_i - \log(r/|w|) + \log(n-r),$$

由此就能导出 n 的有效上界（不应用 Gellfond－Baker 理论是复杂的，如此的常数是比较小的）。又若 $\Delta<0$，引理 4·11 的证明之下导出 $\theta_i=0$，从那里，由(4·12)，对某常数 v_0，

$$|G_n| = |w|\cdot \prod_{i=1}^{s} p_i^{m_i} \leqslant v_0\cdot n.$$

4·3 节的结果及运算仅作较小改变就足以论及这个代替(4·7)的不等式.

然而，存在一种处理这种情形的初等方法，仅用同余就保证能做. 我们定义下列特别“对称递归”. α,β 的定义如 4·2 节，设 d 是 Δ 的无平方部分，令，

$$R_n = \frac{\alpha_n - \beta_n}{\alpha-\beta}, \quad S_n = \alpha^n + \beta^n,$$

又对 $d=-1$，

$$T_n^{\pm} = (1 \pm \sqrt{-1}\cdot\alpha^n + (1 \mp \sqrt{-1})\cdot\beta^n,$$

又对 $d=-3$（对 $\rho=\frac{1}{2}\cdot(1+\sqrt{-3})$，满足 $\omega=\rho$ 或 $\bar{\rho}$），

$$U_n(\omega) = (1+\omega)\cdot\alpha^n + (1+\bar{\omega})\cdot\beta^n,$$

$$V_n(\omega)=\omega\cdot\alpha^n+\omega\cdot\beta^n,$$

其中所有 $n\in Z$. 注意到

$$T_n^+\cdot T_n^-=2\cdot S_{2n},\ U_n(\omega)\cdot U_n(\bar{\omega})\cdot R_n=3\cdot R_{3n},$$

$$V_n(\omega)\cdot V_n(\bar{\omega})\cdot S_n=S_{3n}.$$

便有下面引理. 我们假定 $\mathrm{ord}_p(\theta)\geqslant 0$.

引理 4·11　若 θ 仅有有限多个非零 p - adic 数字, 则存在一个 $r\in N_0$ 和一个 $k\in Q$, 使得

$$G_n=k\cdot R_{n-r},\ 或\ G_n=k\cdot S_{n-r},\ 或(若\ d=-1)$$

$$G_n=k\cdot T_n^{\pm},\ 或(若\ d=-3)G_n=k\cdot U_n(\omega)或\ k\cdot V_n(\omega),$$

其中 $\omega=\rho$ 或 $\bar{\rho}$. 此外, 若 $\Delta<0$, 则 $r=0$.

证明　由 $\mathrm{ord}_p(\theta)\geqslant 0$, 对某 $r\in N_0$, 有 $\theta=r$. 由 θ 的定义, 得

$$\log_p\left[\frac{\alpha}{\beta}\right]^r\cdot\left[\frac{\lambda}{\mu}\right]=0.$$

因此 $\eta=(\beta/\alpha)^r\cdot(\mu/\lambda)$ 是一个单位根. 由此可写出

$$G_n=\lambda\cdot\alpha^r\cdot[\alpha^{n-r}+\eta\cdot\beta^{n-r}].$$

首先设 $B=\pm 1$, 则 $\Delta>0$ 且

$$G_0=\lambda\cdot\alpha^r\cdot[\alpha^{-r}\pm\beta^{-r}]=\pm\lambda\cdot\alpha^r[\alpha^r\pm\beta^r],$$

$$G_1=\lambda\cdot\alpha^r\cdot[\alpha^{1-r}\pm\beta^{1-r}]=\pm\lambda\cdot\alpha^r[\alpha^{r-1}\pm\beta^{r-1}].$$

注意到

$$(\alpha^{r-1}+\beta^{r-1},\alpha^r+\beta^r)=(2,\alpha+\beta)=(1)\text{或}(2),$$

$$(\alpha^{r-1}-\beta^{r-1},\alpha^r-\beta^r)=(\alpha-\beta).$$

由$(G_0,G_1)=1$，分别得$\pm\lambda\cdot\alpha^r=1$，$\frac{1}{2}$或$1/(\alpha-\beta)$. 由此便导出结论.

其次假定$|B|\geqslant 2$定则

$$G_0\cdot B\cdot(\eta\cdot\alpha^{r-1}+\beta^{r-1})=G_1\cdot(\eta\cdot\alpha^r+\beta^r).$$

因为$(B,G_1)=1$，故有$\alpha\cdot\beta|\eta\alpha^r\pm\beta^r$. 由$(A,B)=1$，有$(\alpha,\beta)=(1)$，由$\alpha|\beta^r$，则导出$\theta=r=0$，故$G_0=\lambda\cdot(1+\eta)\in Z$. 现在容易得到结论. 因为对所有$d$，$\eta$仅有可能是$\pm 1$，再者，当$d=-1$时，有$\eta=\pm\sqrt{-1}$，当$d=-3$时，$\eta=\pm\rho$或$\pm\bar{\rho}$.

在引理 4·11 的情形，对(4·1)可作如下处理. 引理 4·10 表明，如同由引理 4·2 和定理 4·4 导出的，使得$m\cdot p^t|G_n$的最小下标$n=g(m\cdot p^t)>0$指数t增长，G_n指数n也增长. 因此，$G_{g(m\cdot p^t)}$指数t双倍增长. 这就导出，当m_i扩充到无限时，$a=w\cdot p_1^{m_1}\cdots p_s^{m_s}$不能继续满足$G_{g(a)}$. 由此，若$p_1^{m_1}\cdots p_s^{m_s}$足够大，则存在一个素数$q$使得$q|G_{g(a)}$但$q\nmid a$. 现在，序列$\{R_n\}$，$\{S_n\}$有特别的可除性性质，有如

$R_n|R_m$当且仅当$n|m$，

$S_n|S_{kn}$，当k为奇数时，

$ord_2(S_n) \leqslant ord_2(S_3)$，对所有 $n \geqslant 1$.

利用这种性质可证明，每当 $a \mid G_n$ 时，$q \mid G_n$. 这就给出(4·1)解的一个上界. 因为对那些解，$a \mid G_n$ 但 $q \nmid G_n$. 我们给出两个例子.

例 设 $A=16$, $B=1$, $G_0=1$, $G_1=8$, $w=1$, $p_1=2$, $p_2=11$，则 $\alpha=8+3\sqrt{7}$, $\beta=8-3\sqrt{7}$, $\lambda=\mu=\frac{1}{2}$，所以 λ/μ 是一个单位根. 因此 $\theta_1=\theta_2=0$. 注意这儿有类型 S_n 的序列. 我们有

n	-3	-2	-1	0	1	2	3
G_n	2024	127	8	1	8	127	2024
$G_n(\bmod 16)$	8	-1	8	1	8	-1	8
$G_n(\bmod 11)$	0	6	8	1	8	6	0
$G_n(\bmod 11^2)$	88	6	8	1	8	6	88
$G_n(\bmod 23)$	0	12	8	1	8	12	0

由此表导出，按照 n 是偶数或奇数，对应 $ord_2(G)=0$ 或 3，而 $ord_{11}(G_n)>0$ 当且仅当 $n\equiv 3(\bmod 6)$. 这也可从引理 4·10 导出，即产生：若 $ord_2(G_n)\geqslant 1$(此恰好对奇数 n 发生)，则 $ord_2(G_n)=3+ord_2(n)=3$. 进而，若 $ord_{11}(G_n)\geqslant 1$(此正好当 $n\equiv 3(\bmod 6)$时发生)，则 $ord_{11}=1+ord_{11}(n)$(例如，$ord_{11}(G_{33}=2$，但 $ord_{11}(G_{11})=0$).

现在，$G_3 \mid G_{3k}$ 对所有奇数 k 成立. 注意 G_3 恰有 3 个因子 2 以及 1 个因子 11，但它比 $2^3\cdot 11=88$ 大. 因此存在一个素数 q 与 2 和 11 不同，使得每当 $11 \mid G_n$ 时，$q \mid G_n$，因此 $G_n=2^{m_1}\cdot 11^{m_2}$没有满足 $m_2\neq 0$ 的解，所以剩下的仅有三个解：$n=-1$,

0,1. 注意知道 q 的确切的值不是必要的. 在此情形 q 的值是 23, 事实上容易直接地证明 $23|G_n$ 当且仅当 $n\equiv3(\mathrm{mod}6)$.

例 设 $A=5, B=13, G_0=G_1=1$. 则 $\Delta=-27, \alpha=1+3\cdot\rho, \lambda=(1+\rho)/3$, 则 $\lambda/\bar{\lambda}=\rho$ 是一个单位根, 因此 $\theta=0$. 我们要解 $G_n=\pm2^m$. 序列 $G_n=\lambda\cdot\alpha^n+\bar{\lambda}\bar{\alpha}^n$ 通过 $G_n\cdot H_n\cdot R_n=R_{3n}/3$ 而与序列 $H_n=\bar{\lambda}\cdot\alpha^n+\lambda\cdot\alpha^{-n}$和序列 $R_n=(\alpha^n-\alpha^{-n})/(\alpha-\bar{\alpha})$是相关的. 因为 R_n 有着优美的可除性性质, 我们得到关于 G_n 和 H_n 的素约数方面的有用资料. 我们发现:

n	0	1	2	3	4	5	6	7	8
G_n	1	1	-8	-53	-161	-116	1513	9073	25696
H_n	1	4	7	-17	-176	-659	-1007	3532	30751
R_n	0	1	5	12	-5	-181	-840	-1847	1685

现在, $G_n\equiv0(\mathrm{mod}16)$当且仅当 $n\equiv8(\mathrm{mod}12)$(引理 4·10 导出: 若 $\mathrm{ord}_2(G_n)\geqslant2$(这当 $n\equiv2(\mathrm{mod}3)$时恰好发生), 则 $\mathrm{ord}_2(G_n)=2+\mathrm{ord}_2(n)$), $H_n\equiv0(\mathrm{mod}16)$当且仅当 $n\equiv4(\mathrm{mod}12)$, 而 $R_n\equiv0(\mathrm{mod}16)$当且仅当 $n\equiv0(\mathrm{mod}12)$. 注意到 $G_4\cdot H_4\cdot R_4=R_{12}/3=-2^4\cdot5\cdot7\cdot11\cdot23$. 考虑这一连串模 5, 7, 11 和 23, 我们发现对所有 $n\equiv0(\mathrm{mod}4)$, $2^4\cdot7\cdot11\cdot23|G_n\cdot H_n$, 而事实上每当 $16|G_n$ 时, $11|G_n$. 因此, $G_n=\pm2^m$ 蕴含 $m\leqslant3$. 由 4·3 节导出如何解 $|G_n|\leqslant8$.

注意上面叙述的过程时常被应用于论及如同引理 4·11 的情况. 这由引理 4·10 来保证.

从现在起我们这样假定, 对所有 $i=1,\cdots,s$, $\mathrm{ord}_{p_i}(\theta_i)\geqslant0$,

而 θ_i 的无限多个 p_i - adic 数字 $u_{i,t}$ 不为零.

4·7 双曲线型情形的简化运算

首先对 $\Delta>0$ 的情形给出简化运算(运算 p, 看图表 6). 其依据仅是引理 4·10 和推论 4·3. 设 N 是关于(4·1)的解 n, $m_1, \cdots, m_s$ 的关于 n 的上界. 例如, 象定理 4·9 中 N [illegible]

图表 6. 运算 P(当 $\Delta>0$ 时降低(4.1)给出的上界)

<u>Input</u>: $\alpha, \beta, \lambda, \mu, w, p_1, \cdots, p_s, N$.

<u>Output</u>: new, reduced upper bounds M_i for m_i for $i=1, \cdots, s$, and N' for n

(i) (initialization) Choose an $n_0 \geqslant 0$ such that

$n_0 > \log|\mu/\lambda| / \log|\alpha/\beta|$; $r := |\lambda| - |\mu| \cdot |\alpha/\beta|^{-n_0}$;

$$\left.\begin{aligned} g_i &:= \mathrm{ord}_{p_i}(\lambda) + \mathrm{ord}_{p_i}(\log_{p_i}(\alpha/\beta)) \\ h_i &:= \mathrm{ord}_{p_i}(\lambda) + \begin{cases} 3/2 & \text{if } p_i = 2 \\ 1 & \text{if } p_i = 3 \\ 1/2 & \text{if } p_i \geqslant 5 \end{cases} \end{aligned}\right\} \text{for } i = 1, \cdots, s;$$

$g := r/|w| \cdot \prod_{i=1}^{s} p_i^{g_i}$; $N_0 := N$;

(ii) (computation of the θ_i's) Compute for $i=1, \cdots, s$ the first r_i p_i - adic digits u of

$$\theta_i = -\log_{p_i}\left(\frac{-\lambda}{\mu}\right) / \log_{p_i}\left(\frac{\alpha}{\beta}\right) = \sum_{t=0}^{\infty} u_{i,t} p_i^t,$$

where r_i is so large that $p_i^{r_i} \geqslant N_0$ and $u_{i,r_i} \neq 0$;

(iii) (further initialization, start outer loop) $s_{i,0} := r_i + 1$ for $i = 1, \ldots, s$; $j := 1$;

(iv) (start inner loop) $i := 1$; $k_i :=$ <u>.false.</u>;

(v) (computation of the new bounds for m_i, terminate inner loop)

```
s_{i,j} := min( s ∈ N_0 | p_i^s ≥ N_{j-1} and u_{i,s} ≠ 0 );
if s_{i,j} < s_{i,j-1}
    then k_j := .true.;
if i < s
    then i := i + 1; goto(v);
(vi) (computation of the new bound for n, terminate outer loop)
    N_j := min (N_{j-1}, [ Σ_{i=1} s_{i,j} logp_i - log g ]/log|α|);
    if N_j ≥ n_0 and K
        then j := j + 1; goto(iv);
        else N' := max(N_j, n_0);
            M_i := max(h_i, g_i + s_{i,j}) for i = 1, ⋯, s; stop.
```

定理 4·12　满足上面所有假设，运算 p 终止．满足 $\Delta>0$ 的方程(4·1)没有满足 $N'\leqslant n<N$ 及对 $i=1,\cdots,s$, $m_i>M_i$ 的解．

证明　因为已假定 θ_i 的 p_i－adic 展式是无限的，故存在 r_i 满足所需性质．显然，$s_{i,1}\leqslant r_i<s_{i,0}$，且 $N_j\leqslant N_{j-1}$．因此对所有 $j\geqslant 1$, $s_{i,j}\leqslant s_{i,j-1}$ 成立．因为 $s_{i,j}\geqslant 0$，故存在一个 j，使得 $N_j\leqslant n_0$，或者对所有 $i=1,\cdots,s$, $s_{i,j}=s_{i,j-1}$ 成立．在运算终止的两种情形的后者，k_j 仍是不成立的．我们用关于 j 的归纳法证明，$m_i\leqslant g_i+s_{i,j}$ 对 $i=1,\cdots,s$ 成立，$n<N_j$ 对所有 j 成立．对 $j=0$, $n<N_0$ 是显然的．假定对某 $j\geqslant 1$, $n<N_{j-1}$．假定存在一个 i，使得 $m_i>g_i+s_{i,j}$．由引理 4·10，有

$$\mathrm{ord}_{p_i}(n-\theta_i)=m_i-g_i\geqslant s_{i,j}+1.$$

由 $u_{i,s_{i,j}}\neq 0$，因此

$$n \geqslant \sum_{t=0}^{a_{i,j}} u_{i,t} \cdot p^t \geqslant p^{a_{i,j}} \geqslant N_{j-1},$$

这与我们的假设矛盾.因此,$m_i \leqslant g_i + s_{i,j}$对 $i=1,\cdots,s$ 成立.则从推论 4·3 导出

$$n < \left[\sum_{i=1}^{s}(g_i + s_{i,j}) \cdot \log p_i - \log(r/|w|)\right]/\log|\alpha|.$$

因此 $n < N_j$.

注释 1 一般地,我们期待 $p_i^{s_{i,j}}$ 不要比 N_j 大得多,即没有太多的 θ_i 的相邻 p_i - adic 数字是零.则 N_j 大约如 $\log N_{j-1}$ 那么大.实际上,运算常在第三或第四步终止,接近于最大解.计算时间是多项式在 s 过程中,运算的瓶颈口是 p_i - adic 对数的计算.

注释 2 Petho[91]对 $s=1$ 给出不同的简化运算.他对素数 p_i 计算函数 $g(u)$,此函数定义为当最小下标 $n \geqslant 0$ 使得 $G_n \neq 0$ 且 $p_i^u | G_n$ 的时候 $u \in N$.注意到若 p_i - adic 极限 $\lim\limits_{n\to\infty} g(u)$ 存在,则由引理 4·10,其极限值为 θ_i.

注释 3 若 $B = \pm 1$(因此 $\Delta > 0$),我们可用递归公式

$$G_{n-1} = A \cdot B \cdot G_n - B \cdot G_{n+1}, \quad n = 0, -1, -2, \cdots$$

扩充数到$\{G_n\}_{n=0}^{\infty}$到负的下标(参见(4·3)).则(4·5)对 $n<0$ 也成立.我们可对 $n \in Z$ 解方程(4·1)而不必限制 n 是非负的.两次运用运算 p:一次对$\{G_n\}_{n=0}^{\infty}$,一次对由 $G_n' = G_{-n}$的序列$\{G_n'\}_{n=0}^{\infty}$.注意到 $G_n' = B^n \cdot [\mu \cdot \alpha^n + \lambda \cdot \beta^n]$,且

$$\theta_i' = -\frac{\log_{p_i}(-\mu/\lambda)}{\log_{p_i}(\alpha/\beta)}$$

$$+\frac{\log_{p_i}(-\lambda/\mu)}{\log_{p_i}(\alpha/\beta)} \doteq -\theta_i, i=1,\cdots,s.$$

现在，我们可以更换两次应用运算 p 的做法，使得能用于所有 $n \in Z$，如下所述．若用 $|n|$ 代替 n，引理 4·8 和 4·10 保持正确．在定理 4·9 中，n_0 的下界需换成

$$n_0 > \max[2, |\log|\mu/\lambda||/\log|\alpha/\beta|, |\log|\lambda/\mu||/\log|\alpha/\beta|],$$

而 r 换成

$$r = \min[|\lambda| - |\mu| \cdot \alpha/\beta|^{-n_0}, |\mu| - |\lambda| \cdot |\alpha/\beta|^{-n_0}].$$

运算 p 的步骤(i)必须作类似的更改．进而，在步骤(ii)中，r_i 的选择需大得使

当 $p_i \neq 2$，则 $p_i^{r_i} \geqslant N_0$ 且 $u_{i,r_i} \neq 0, u_{i,r_i} \neq p-1$；

否则　$p_i^{r_i-1} \geqslant N_0$ 且 $u_{i,r_i} \neq u_{i,r_i-1}$．

在步骤(v)中也需对 $s_{i,j}$ 作类似地更改．有了这些改变，定理 4·12 对于用 $|n|$ 代替 n 保持成立．

我们用一个例子来结束本节．

例　设 $A=6, B=1, G_0=1, G_1=4, w=1, p_1=2, p_2=1$．则 $\alpha=3+2\cdot\sqrt{2}, \beta=3-2\cdot\sqrt{2}, \lambda=(1+2\cdot\sqrt{2})/4\cdot\sqrt{2}, \mu=(-1+2\cdot\sqrt{2})/4\cdot\sqrt{2}$，又 $\Delta=32$．对 $n_0 \doteq e^{60}=1.142\times10^{26}$ 我们找到 $C_4 < 2.49\times10^{20}$．对上述注释了的更改，我们得到 $r>0.323$，$C_5<1.76$，$C_6<2.62\times10^{26}$，$C_5\cdot C_6<4.62\times10^{26}$．因此 $G_n \doteq 2^{m_1}\cdot$

11^{m_2}的所有解满足$|n|<4.62\times10^{26}$, $\max(m_1,m_2)<2.62\cdot10^{26}$. 我们逐步地完成简化运算 p.（我们将 p－adic 数$\sum_{i=0} u_i\cdot p^i$写成 $0.u_0u_1u_2\cdots$，若 $p>10$，我们用符号 A，B，C… 表示比 9 大的数字）.

(i) $n_0=2, r=0.303, g_1=0, g_1=1, g>0.0275,$

$h_1=-1, h_2=\frac{1}{2}, N_0=4.62\times10^{26}$.

(ii) $\theta_1=0.10111\ 10111\ 01000\ 11100\ 10100\ 01001\ 10001\ 10010$
$00001\ 11101\ 01000\ 10000\ 01001\ 10011\ 10101\ 01101$
$11100\ 01011\ 00001\ 11010\ 00011\ 01001\ 01010\ 00101$
$10001\ 01011\ 00000\ 11001\ 01011\ 11101\ 10100\ 01011$
$001\cdots$,

$\theta_2=0.A9359\ 05530\ 7330A\ 1A223\ 96230\ 3A006\ A3366$
$83368\ 8270\cdots$,

故 $r_1=90$(因 $u_{1,89}=1, u_{1,90}=0, 2^{89}>N_0$)

$r_2=29$(因 $u_{2,29}=6, 11^{29}>N_0$).

(iii) $s_{1,0}=91, s_{2,0}=30$.

(v)－(vi) $s_{1,1}=90, s_{2,1}=29, k_1=.ture., N_1<76.9$;

(v)－(vi) $s_{1,2}=10, s_{2,2}=2, k_2=.ture., N_2<8.7$;

(v)－(vi) $s_{1,3}=6, s_{2,3}=2, k_3=.ture., N_3<5.8$;

(v)－(vi) $s_{1,4}=6, s_{2,4}=2, k_4=.fals., N_4<5.8$.

因此$|n|\leqslant5, m_1\leqslant6, m_2\leqslant2$. 我们有

n	−5	−4	−3	−2	−1	0	1	2	3	4	5
G_n	2174	373	64	11	2	1	4	23	134	781	4552

因此有 5 个解：满足 $n=-3,-2,-1,0,1$.

4·8 椭圆型情形的简化运算

现在介绍(4·1)在 $\Delta<0$ 的情况下,降低其解的上界的运算.想法是交替应用运算 p 以及运算 H 或 I 中总有一个.设 N 是 n 的一个上界,例如,象定理 4·9 中 $n=C_7$.由引理 4·6,4·7 及定理 4·12 的证明立即导出下面定理.

定理 4·13　运算 C(见图表 7)终止,方程(4·1)在 $\Delta<0$ 时,没有满足 $N^*<n<N$ 及 $m_i>M_i(i=1,\cdots,s)$的解.除非那些疵点通过运算.

图表 7. 运算 C(在 $\Delta<0$ 的情形降低(4.1)的上界)

Input: $\alpha, \beta, \lambda, \mu, w, p_1, \cdots, p_s, N$.

Output: new, reduced upper bounds N^* for n, and M_i for m_i for $i=1,\cdots,s$.

(i) (initialization) $N_0:=[N]$; $j:=1$;

$$\left.\begin{array}{l} g_i:=\text{ord}_{p_i}(\lambda)+\text{ord}_{p_i}(\log_{p_i}(\alpha/\beta)) \\ h_i:=\text{ord}_{p_i}(\lambda)+\begin{cases}3/2 \text{ if } p_i=2\\ 1 \text{ if } p_i=3\\ 1/2 \text{ if } p_i\geqslant 5\end{cases}\end{array}\right\} \text{for } i=1,\cdots,s;$$

(ii) (computation of the θ'_is, φ, ψ) Compute for $i=1,\cdots,s$ the first r_i p_i-adic digis $u_{i,t}$ of

$$\theta_i=-\log_{p_i}\left(\frac{-\lambda}{\mu}\right)/\log_{p_i}\left(\frac{\alpha}{\beta}\right)=\sum_{t=0}^{\infty}u_{i,t}\cdot p_i^t,$$

where r_i is so large that $p_i^{r_i}\geqslant N_0$ and $u_{i,r_i}\neq 0$; compute $\psi=\log(-\lambda/\mu)/2\pi i$, and the continued fraction

$$|\varphi|=\left|\frac{1}{2\pi i}\cdot\log(\alpha/\beta)\right|=[0,a_1,\cdots,a_{t0},\cdots]$$

wich the convergents p_i/q_i for $i=1,\cdots,\iota_0$, where ι_0 is so large that $q_{\iota_0-1} \leqslant N_0 < q_{\iota_0}$ if $\psi=0$; $q_{\iota_0} > 4\cdot N_0$ and $\| q_{\iota_0} \| > 2\cdot N_0/q_{\iota_0}$ if $\psi \neq 0$ and such ι_0 can be found in a reasonable amount of time, $q_{\iota_0} > 4\cdot N_0$ otherwise;

(iii) (one step of Algorithm P) For $i=1,\ldots,s$ put $M_{i,j} := \max\{h_i, g_i + \min\{s \in N_0 \mid p_i^s \geqslant N_{j-1}$ and $u_{i,s} \neq 0\}\}$;

(iv) (one step of Algorithm Hor I)

if $\psi=0$

then $A := \max(a_1,\cdots,a_{\iota_j-1})$; $v := |w|\cdot\prod\limits_{i=1} p_i^{M_{i,j}}$;

choose $n_0 \geqslant 2/\log B$ such that $B^{n_0/2}/n_0 \geqslant v/2\cdot|\mu|$;

compute the largest integer N_j such that

$$B^{N_j/2}/N_j \leqslant (A+2)\cdot v/4\cdot|\mu|;$$

$N_j := \max(n_0, N_j)$;

if $N_j < N_{j-1}$ then compute ι_j with $q_{\iota_j-1} \leqslant N_j < q_{\iota_j}$; [illegible]

else if $\| q_{\iota_{j-1}}\cdot\psi \| > 2\cdot N_{j-1}/q_{\iota_{j-1}}$

then $N_j := [2\cdot\log\{q_{\iota_{j-1}}^2\cdot v/4\cdot|\mu|\cdot N_{j-1}\}/\log B]$;

else compute $k \in Z$ with $|k - q_{\iota_{j-1}}\cdot\psi| \leqslant \frac{1}{2}$;

compute $n_0 \in Z, 0 \leqslant n_0 < q_{\iota_{j-1}}$, with

$K + n_0\cdot p_{\iota_{j-1}} = 0 \pmod{q_{\iota_{j-1}}}$;

if $n = n_0$ is a solution of (4.1)

then print an appropriate message;

$N_j := [2\cdot\log\{q_{\iota_{j-1}}\cdot v/|\mu|\}/\log B]$;

if $N_j < N_{j-1}$

then compute the minimal $\iota_j < \iota_{j-1}$ such that $q_{\iota_j} > 4\cdot N_j$ and $\| q_{\iota_j}\cdot\psi \| > 2\cdot N_j/q_{\iota_j}$ (if such ι_j does not exist, choose the minimal ι_j such that $q_{\iota_j} > 4\cdot N_j$); $j := j+1$; goto(iii);

(v) (termination) $N^* := N_{j-1}$; $M_i := M_{i,j}$ for $i=1,\cdots,s$; stop.

例　设 $A=1, B=2, G_0=2, G_1=3$，则 $\Delta=-7, \alpha=(1+$

$\sqrt{-7})/2$, $\lambda=(2+\sqrt{-7})/\sqrt{-7}$. 设 $w=\pm1$, $p_1=3$, $p_2=7$. 满足 $n_0=2$, 我们有下面结果: $C_4<6.40\times10^{16}$, $C_3=9.14\times10^{29}$, C_7 7.42×10^{30}, $\max(C_{8,1}, C_{8,2}<2.30\times10^{22}$. 进而, $g_1=1$, $g_2=0$, $h_1=1$, $h_2=0$. 由定理 4·9, 我们可选择 $N_0=7.42\times10^{30}$. 我们有

$$\begin{aligned}\varphi &= [\pi-\operatorname{arctg}(\sqrt{7}/3)]/2\pi\\ &=[0,2,1,1,2,16,6,1,2,2,13,1,1,3,1,1,2,1,2,1,\\ &\quad 1,1,1,1,9,2,1,2,1,7,1,6269,4,3,1,1,50,2,1,\\ &\quad 6,1,1,2,1,1,7,1,61,1,12,3,7,4,7,3121,1,21,\\ &\quad 2,1,7,\cdots],\end{aligned}$$

$$\begin{aligned}\psi &= [\pi-\operatorname{arctg}(4\cdot\sqrt{7}/3)]/2\pi\\ &=0.29396\ 28336\ 99645\ 40267\ 89566\ 60520\ 01908\ 06203\cdots,\end{aligned}$$

$$\begin{aligned}\theta_1 &= 0.20010\ 12210\ 00011\ 02102\ 00211\ 00222\ 02220\ 12021\ 10020\ 20202\\ &\quad 21102\ 00121\ 01000\ 01002\ 11100\ 20122\ 11111\ 22202\ 21021\ 02212\\ &\quad 2200\cdots,\end{aligned}$$

$$\begin{aligned}\theta_2 &= 0.32542\ 12042\ 43561\ 34020\ 61561\ 13452\ 10116\ 33152\ 25336\ 45044\\ &\quad 11254\ 55033\cdots\end{aligned}$$

现在我们选择 $\iota_0=61$, 因为

$$q_{61}=142\ 51183\ 31142\ 44361\ 19375\ 51238\ 81743>4\cdot N_0$$

且 $\|q_{61}\cdot\psi\|=0.24487\cdots>2\cdot N_0/q_{61}=0.104\cdots$. 我们有 $M_{1,1}=67$, $M_{2,1}=37$, 并找到 $N_1=637$. 其次我们取 $\iota_2=6$, 因为 $q_6=1291>4\times74$, $\|q_6\cdot\psi\|=0.49398>2\times74/1291$. 就有 $M_{1,3}=6$, $M_{2,3}=3$, 且我们找到 $N_3=60$. 下一步我们发现没有改进. 因为 $n\leqslant60$, $m_1\leqslant6$, $m_2\leqslant3$. 理所当然的直接计算来检验, $G_n=\pm3^{m_1}\cdot7^{m_2}$ 仅有下列 6 个解: $G_1=3$, $G_2=-1$, $G_3=-7$, $G_5=3^2$, $G_7=1$, $G_{17}=3^2\cdot7^2$.

4·9 广义 Ramanujan－Nagell 方程

前节的简化运算最有趣的应用似乎是解广义 Ramanujan－Nagell 方程(4·2). 设 k 是非零整数，$p_1, \cdots, p_s$ 是不同素数. 则我们要求对所有非负整数 $x, z_1, \cdots, z_s$，满足

$$x^2 + k = \prod_{i=1}^{s} p_i^{z_i}.$$

首先注意到每当 $-k$ 是平方非剩余$(\bmod p_i)$时，$z_i = 0$. 因此我们假定对所有 i 不全是此情形. 设当 $i = 1, \cdots, t$ 时，$p_i | k$，且当 $i = t+1, \cdots s$ 时，$p_i \nmid k$. 设对 $i = 1, \cdots, r$，$\mathrm{ord}_{p_i}(k)$是奇数而对 $i = r+1, \cdots, t$，$\mathrm{ord}_{p_i}(k)$是偶数. 对 $i = 1, \cdots, t$，用 p_i 的足够大的幂除，(4·2)简化成有限方程

$$D_0 x_1^2 + k_1 = \prod_{i=r+1}^{s} p_i^{z_i'}, \tag{4·13}$$

满足对 $i = 1, \cdots, s$，$p_i \nmid k_1$，且 D_0 仅由 $p_1, \cdots, p_r$ 组成，D_0 无平方因子. 对 $i = r+1, \cdots, s$，我们将 z_i'的 2^{s-r}个组合按 z_i'的奇偶性分类. 假定对 $i = r+1, \cdots, u$，z_i'是奇数，对 $i = u+1, \cdots, s$，z_i'是偶数. 令

$$y = \prod_{i=r+1}^{u} p_i^{(z_i'-1)/2} \cdot \prod_{i=u+1}^{s} p_i^{z_i'/2} \tag{4·14}$$

则由(4·13)，有

$$D_0 \cdot x_1^2 - [\prod_{i=r+1}^{u} p_i] \cdot y^2 = -k_1 \tag{4·15}$$

令 $D = D_0 \prod_{i=r+1}^{u} p_i$，则(4·14)和(4·15)导出

$$\begin{cases} v^2 - D \cdot w^2 = k_2 \\ v = \prod_{i=r+1}^{s} p_i^{m_i} \end{cases} \tag{4·16}$$

满足 $v = y \cdot \prod_{i=r+1}^{u} p_i$，$w = x_1$，$k_2 = k_1 \cdot \prod_{i=r+1}^{u} p_i$，且又有

$$\begin{cases} v^2 - D \cdot w^2 = k_2 \\ w = \prod_{i=r+1}^{s} p_i^{m_i} \end{cases} \tag{4·17}$$

满足 $v = D_0 \cdot x_1$，$w = y$，$k_2 = -k_1 \cdot D_0$. 我们将在(4·16)或(4·17)继续做下去，多半是合适的(例如总有较小$|k_2|$).

若 $D = 1$，则(4·16)和(4·17)是平凡的. 故假定 $D > 1$. 设 ε 是 $Z + \sqrt{D} \cdot Z$ 中满足 $\varepsilon > 1$ 的最小单位. 如所熟知，方程 $v^2 - D \cdot w^2 = k_2$ 的解 v, w 分别属于有关解的有限类数. 设 T 是这样的类，对于 $r = 1, \cdots, T$，选择解 $v_{r,0}$，$w_{r,0}$的第 r 类使得 $r_t = v_{r,0} + w_{r,0} \cdot \sqrt{D} > 1$ 最小，则 $v^2 - D \cdot w^2 = k_2$ 的所有解便由 $v = \pm v_{r,n'}$，$w = \pm w_{r,n'}$给出. 对 $n \in Z$，满足

$$\begin{cases} v_{r,n} = [r_r \cdot \varepsilon^n + r_r' \cdot \varepsilon^{-n}]/2 \\ w_{r,n} = [r_r \cdot \varepsilon^n - r_r' \cdot \varepsilon^{-n}]/2 \cdot \sqrt{D} \end{cases} \tag{4·18}$$

其中 $r'_t = v_{r,0} - w_{r,0} \cdot \sqrt{D}$. 即 $\{v_{r,n}\}_{n=-\infty}^{\infty}$ 及 $\{w_{r,n}\}_{n=-\infty}^{\infty}$ 为线性双递归序列. 现在，(4·16)和(4·17)简化为 T 个类型(4·1)的

方程. 若 $k_2=1$, 则 $T=1$, $r_1=\varepsilon$, $r_1'=\varepsilon^{-1}$. 若 $k_2|2\cdot D$, $k_2\neq 1$, 则容易证明, $r_r^2=|k_2|\cdot\varepsilon$, $r_r'^2=|k_2|\cdot\varepsilon^{-1}$, 因此

$$v_{r,n}=\sqrt{|k_2|}\cdot\left[\left[r_r/\sqrt{|k_2|}\right]^{2n+1}+\left[r_r'/\sqrt{|k_2|}\right]^{2n+1}\right]/2,$$

$$w_{r,n}=\sqrt{|k_2|}\cdot\left[\left[r_r/\sqrt{|k_2|}\right]^{2n+1}-\left[r_r'/\sqrt{|k_2|}\right]^{2n+1}\right]/2\cdot\sqrt{D},$$

在两种情形,(4·16)和(4·17)都可用初等方法求解(在4·6节); 我们感兴趣的是 Størmer[113], Mahler[75], Lehmer[67], Rumsey 和 Posner[100]和 Mignotte[80]等人的工作). 若 $k_2\nmid 2\cdot D$, 则我们的简化运算总可用于方程 $v_{r,n}=\prod_{i=r+1}^{s}p_i^{m_i}$, $w_{r,n}=\prod_{i=r+1}^{s}p_i^{m_i}$ 的一个. 注意 n 容许是非负的, 因为 $B=\pm 1$, 所以我们可运用 4·7 节注释 3 的更改运算.

例如我们有解(4·2)的一个完整程序. 如所熟知, 怎样能用$\sqrt{D}$的连分数运算来计算出单位 ε 以及 $r=1,\cdots,T$ 时的最小解 $v_{r,0}$, $w_{r,0}$. 我们用一个例子来结束本节. 此例子扩充了 Nagell[86](也由不少其他人证明了的)关于基本 Ramanujan - Nagell 方程 $x^2+7=2^z$ 的结果.

定理 4·14　使 x^2+7 没有比 20 大的素因子的非负整数 x 只有 16 个, 如下表.

x	x^2+7	x	x^2+7	x	x^2+7
0	7	7	$56=2^3\cdot 7$	31	$968=2^3\cdot 11^2$
1	$8=2^3$	9	$88=2^3\cdot 11$	35	$1232=2^4\cdot 7\cdot 11$
2	11	11	$128=2^7$	53	$2816=2^8\cdot 11$
3	$16=2^4$	13	$176=2^4\cdot 11$	75	$5632=2^9\cdot 11$
5	$32=2^5$	21	$448=2^6\cdot 7$	181	$32768=2^{15}$
				273	$74536=2^3\cdot 7\cdot 11^3$

证明　因为 -7 是模 3, 5, 13, 17 和 19 的平方非剩余，左边仅有素数 2, 7 和 11. 唯一因子 7 能出现在 x^2+7 中，因此我们要解两个方程

$$x^2+7=2^{z_1}\cdot 11^{z_2} \tag{4·19}$$

$$x^2+7=7\cdot 2^{z_1}\cdot 11^{z_2} \tag{4·20}$$

方程(4·20)可用初等方法来解. 我们分为四种情形，每种情形导出一个类型的方程

$$y^2-Dz^2=c$$

满足 $c\mid 2\cdot D$，且或者 y 或者 z 仅由因数 2 和 11 组成. 我们有：

(1) z_1 是偶数，z_2 是偶数，$y=2^{z_1/2}\cdot 11^{z_2/2}$，$z=x/7$，$c=1$，D

$=7$;

(ii) z_1 是奇数，z_2 是偶数，$y=2^{(z_1+1)/2}\cdot 11^{z_2/2}$，$z=x/7$，$c=2$，$D=14$；

(iii) z_1 是偶数，z_2 是奇数，$y=x$，$z=2^{z_1/2}\cdot 11^{(z_2-1)/2}$，$c=-7$，$D=77$；

(iv) z_1 是奇数，z_2 是奇数，$y=x$，$z=2^{(z_1-1)/2}\cdot 11^{(z_2-1)/2}$，$c=-7$，$D=154$.

在4·5节第一例子我们已做出情形(i). 我们把其他情形留给读者.

方程(4·19)可用简化方法来解. 我们再分四种情形，每一情形导出形如

$$y^2-D\cdot z^2=c$$

的一个方程，满足 z 仅由因子2和11组成. 有

(i) z_1，z_2 都是偶数，$y=x$，$z=2^{z_1/2}\cdot 11^{z_2/2}$，$c=-7$，$D=2$；

(ii) z_1 是奇数，z_2 是偶数，$y=x$，$z=2^{(z_1-1)/2}\cdot 11^{z_2/2}$，$c=-7$，$D=2$；

(iii) z_1 是偶数，z_2 是奇数，$y=x$，$z=2^{z_1/2}\cdot 11^{(z_2-1)/2}$，$c=-7$，$D=11$；

(iv) z_1，z_2 都是奇数，$y=x$，$z=2^{(z_1-1)/2}\cdot 11^{(z_2-1)/2}$，$c=-7$，$D=22$.

情形(i)是平凡的，其余三种情形，每种导出一个类型(4·1)的方程. 在4·7节的例子中我们已作出情形(ii). 依据下面数据，读者应能着手对情形(iii)和(iv)完成运算 P，从而完成证明. 在这些情形，$N<10^{30}$是正确上界.

情形(iii)：$\alpha=10+3\cdot\sqrt{11}$，$\lambda=(2+\sqrt{11}/2\cdot\sqrt{11}$，

$\theta_1 = 0.10011\ 01000\ 00110\ 10100\ 00110\ 10110\ 01001\ 11110\ 11011\ 10010\ 00001$
$10110\ 10111\ 10100\ 00110\ 01101\ 01010\ 10010\ 11101\ 11001\ 10000\ 10010$
$01010\ 11011\ 00010\ 00111\ 01110\ 00101\ 01101\ 01111\ 10101\ 11110\ 10\cdots,$

$\theta_2 = 0.23075\ 76425\ 39004\ 26090\ A92A1\ 03757\ 07314\ 58414\ 7A238\cdots$

情形(iv)：$\alpha = 197 + 42\cdot\sqrt{22}$，$\lambda = (9 + 2\cdot\sqrt{22})/2\cdot\sqrt{22}$，

$\theta_1 = 0.11101\ 01101\ 01110\ 01010\ 10111\ 10001\ 00100\ 00011\ 10000\ 00110$
$10101\ 01100\ 01101\ 01111\ 01101\ 10101\ 01011\ 10100\ 01100\ 11101$
$10011\ 00011\ 00010\ 11110\ 10101\ 01100\ 10011\ 11111\ 01001\ 01110$
$00000\ 01110\ 011\cdots,$

$\theta_2 = 0.6A001\ 68184\ 22921\ 902A0\ 724A4\ 16769\ 45650\ 16482\ 5A6AA\cdots.$

注释　1. 上面证明的计算时间少于 2 秒.

2. 设 $\Phi(X, Y) = aX^2 + bXY + CY^2$ 是整系数二次型，$\Delta = b^2 - 4\cdot a\cdot c$ 可正可负. K 是非零整数，$p_1, \cdots, p_s$ 是不同素数. 注意到

$$4\cdot a\cdot\Phi(X, Y) = (2\cdot a\cdot X + b\cdot Y)^2 - \Delta\cdot Y^2,$$

因此丢番图方程

$$\Phi(X, K) = \prod_{i=1}^{s} p_i^{z_i},$$

$$\Phi\left(X, \prod_{i=1}^{s} p_i^{z_i}\right) = K,$$

其中 $X \neq 0$，$z_1, \cdots, z_s \in N_0$，可以用我们的方法来求解.

4·10　混合的平方指数方程

本节对下面丢番图方程给出运算 C 的一种应用. 设

$$\Phi(X, Y) = a \cdot X^2 + b \cdot X \cdot Y + c \cdot Y^2$$

是整系数二次型，使得 $D = b^2 - 4 \cdot a \cdot c$ 是负的．设 q, v, w 为非零整数，$p_1, \cdots, p_s$ 是不同素数．考虑方程

$$\Phi(X, w \cdot \prod_{i=1}^{s} p_i^{m_i}) = v \cdot q^n, \tag{4·21}$$

其中 X 是整数，$n, m_1 \cdots, m_s \in N_0$．

设 $\beta, \bar{\beta}$ 是 $\Phi(X, 1) = 0$ 的根．h 是 $Q(\sqrt{D})$ 的类数．存在 $a, \pi \in Q(\sqrt{D})$，使得我们有主理想方程 $(\pi) \cdot (\bar{\pi}) = (q^h)$．令 $n = n_1 + h \cdot n_2$，满足 $0 \leqslant n_1 < h$，则 $\Phi(X, Y) = v \cdot q^n$ 等价于有限多个理想方程．

$$(a \cdot X - a \cdot \beta \cdot Y) \cdot (a \cdot X - a \cdot \bar{\beta} \cdot Y) = (\sigma) \cdot (\bar{\sigma}) \cdot (\pi)^{n_2} \cdot (\bar{\pi})^{n_2},$$

满足 $(\sigma) \cdot (\bar{\sigma}) = (a \cdot v \cdot q^{n_1})$．因此有代数数方程

$$\begin{cases} a \cdot X - a \cdot \beta \cdot Y = \gamma \cdot \pi^{n_2} \\ a \cdot X - a \cdot \bar{\beta} \cdot Y = \bar{\gamma} \cdot \bar{\pi}^{n_2}, \end{cases}$$

$$\begin{cases} a \cdot X - a \cdot \beta \cdot Y = \gamma \cdot \bar{\pi}^{n_2} \\ a \cdot X - a \cdot \bar{\beta} \cdot Y = \bar{\gamma} \cdot \pi^{n_2}, \end{cases}$$

其中 γ 是由 σ、单位元以及 $a \cdot X - a \cdot \beta \cdot Y$ 和 $a \cdot X - a \cdot \bar{\beta} Y$ 的公约数组成的．注意对 γ 的选择仅有有限多种可能．因此，(4·21) 等价于有限数方程

$$a\cdot(\bar{\beta}-\beta)\cdot w\cdot\prod_{i=1}^{s}p_i^{m_i}=\gamma\cdot\pi^{n_2}-\bar{\gamma}\cdot\bar{\pi}^{n_2},$$

或者，若设 $\lambda=r/a\cdot(\bar{\beta}-\beta)$，$g_{n_2}=\lambda\cdot\pi^{n_2}+\bar{\lambda}\,\bar{\pi}^{n_2}$，则有

$$G_{n_2}=w\cdot\prod_{i=1}^{s}p_i^{m_i} \tag{4·22}$$

这里，$\{G_{n_2}\}_{n_2=0}^{\infty}$是满足判别式为负的递归数列．因此(4·22)属于类型(4·1)，因此可用4·8节的简化运算来解．

在举例之前我们指出，满足 $D>0$ 的(4·21)用本章的方法是不可解决的．这基于这样的事实：$D>0$ 时 $Q(\sqrt{D})$ 有无限多个单位，因此关于 γ 有无限多可能．另一个一般的方程(4·21)是用 $\prod_{i=1}^{t}p_i^{m}$ 代替 q^n．这个问题用本章的方法也不能解决，这是因为当 $t\geqslant 2$ 时，它导不出一个双递归序列．但此问题通过运用多维逼近方法来论及，正如在第3章及第7章中的应用所介绍的．

最后介绍一个例子．

定理4·15 方程

$$X^2-3^{m_1}\cdot 7^{m_2}\cdot X+2\cdot[3^{m_1}\cdot 7^{m_2}]^2=11\cdot 2^n,$$

$X\in Z$，$n, m_1, m_2\in N_0$，仅有下列24个解：

n	m_1	m_2	X	n	m_1	m_2	X
1	1	0	−1,4	5	2	0	−10,19
1	0	0	−4,5	6	0	0	−26,27
2	0	0	−6,7	7	0	0	−37,38
3	0	1	2,5	7	3	0	2,25
3	1	0	−7,10	11	1	1	−137,158
4	0	1	−6,13	17	2	2	−829,1270

证明　令 $\beta=(1+\sqrt{-7})/2$，则

$$X^2-X\cdot Y+2\cdot Y^2=(X-\beta\cdot Y)\cdot(X-\bar{\beta}\cdot Y).$$

注意 $Q(\sqrt{-7})$ 有类数 1，且

$$2=\frac{1+\sqrt{-7}}{2}\cdot\frac{1-\sqrt{-7}}{2},$$

$$11=(2+\sqrt{-7})\cdot(2-\sqrt{-7}).$$

假定 $\gamma|X-\beta\cdot Y$ 且 $\gamma|X-\bar{\beta}\cdot Y$. 则 $\gamma|(\bar{\beta}-\beta)\cdot Y=-\sqrt{-7}\cdot 3^{m_1}\cdot 7^{m_2}$. 另一方面，$\gamma|11\cdot 2^n$. 由此导出 $\gamma=\pm 1$，因此 $X-\beta\cdot Y$ 与 $X-\bar{\beta}\cdot Y$ 是互素的. 因此有两种可能：

$$X-\beta\cdot Y=\pm(2\pm\sqrt{-7})\cdot\left[\frac{1\pm\sqrt{-7}}{2}\right]^n,$$

$$X-\beta\cdot Y=\pm(2\mp\sqrt{-7})\cdot\left[\frac{1\pm\sqrt{-7}}{2}\right]^n,$$

在每个方程中，第二和第三个 ± 号是独立的. 因此我们需解

$$G_n^{(j)} = \lambda^{(j)} \cdot \beta^n + \bar{\lambda}^{(j)} \cdot \bar{\beta}^n = 3^{m_1} \cdot 7^{m_2}, \quad j = 1, 2$$

满足 $G_{n+1}^{(j)} = G_n^{(j)} - 2 \cdot G_{n-1}^{(j)}$, $j = 1, 2$, 以及 $\lambda^{(1)} = \bar{\lambda}^{(2)} = (2 + \sqrt{-7}/\sqrt{-7}$, 因此 $G_0^{(1)} = G_0^{(2)} = 1$, $G_1^{(1)} = 3$, $G_1^{(2)} = -1$. 注意对于 $i = 1, 2$, 有 $\theta_i^{(1)} = -\theta_i^{(2)}$, 且 $\psi^{(1)} = -\psi^{(2)}$ 对于 $j = 1$, 我们在 4·8 节的例中已解决(4·22). 对于 $j = 2$, 留待读者解(4·22). 这可用 $j = 1$ 的情形所给的数据来做.

注释　上面证明的运算时间少于 3 秒.

第五章　S－整数不等式 $0<x-y<y^{\delta}$

5·1　导言

设 S 是由取自固定有限集 $\{p_1,\cdots,p_s\}$ 的素数所组成的所有正整数集合，其中 $s\geq 2$，并且设 $\delta\in(0,1)$。本章研究丢番图不等式

$$0<x-y<y^{\delta} \tag{5·1}$$

其中 $x,y\in S$。我们给出其解的显示上界，并说明如何运用已在第三章介绍的实情形齐次一维和多维丢番图逼近运算，就任意参数 $p_1,\cdots,p_s,\delta$ 的集合，求出(5·1)的全部解。对 $s=2$，用连分数法(看 3·2 节)。对 $s\geq 3$，我们用 L^3－运算来降低上界(看 3·7)节)。

Tijdeman[116](也可看 Shorey 和 Tijdeman[107]，定理 1·1)证明存在一个仅依赖于 $\max(p_i)$ 的可计算的数 c，使得对满足 $x>y\geq 3$ 的所有 $x,y\in S$，都有

$$x-y>y/(\log y)^{c}.$$

因此，对于(5·1)的任意解，导出关于 x，y 的界。Størmer[113]证明如何用初等方法解 $k=1,2$ 时的方程 $x-y=k$(也可看 Mahler[75]，Lehmer[67])。我们的方法可对任意 $k\in Z$ 解这个方程。对一维情形 $s=2$，Ellison[37]已证明下面结果：对所有但有限多个明显可见的除外，$|2^x-3^y|>\exp[x\cdot(\log 2-1/$

10)] 对一切 $x, y \in N$ 成立. Cijsouw, Korlaar 和 Tijdeman (Stroeker 和 Tijdeman[114]的附录)已求出不等式

$$|p^x - q^y| < p^{\delta \cdot x}$$

在所有素数 p, q 满足 $p < q < 20$ 且 $\delta = \frac{1}{2}$ 时的全部解 $x, y \in N$. 我们要将这些结果扩充到对更多的 p、q 的值以及 $\delta = 0.9$. 此外, 我们对多维情形 $s = 6$, $\{p_1, \cdots, p_6\} = \{2, 3, 5, 7, 11, 13\}$ 以及 $\delta = \frac{1}{2}$, 确定(5·1)的所有解. 有关这方面的结果还可参见文献[47]、[48]、[49], [83]、[84].

在 5·2 节, 我们导出(5·1)的解的上界. 在 5·3 和 5·4 节, 我们分别就一维和多维情形, 给出降低上界的方法, 并就一些例子, 求出显示的上界. 5·5 节包含了数据表.

5·2 解的上界

假定素数的次序是 $p_1 < \cdots < p_s$. 对于(5·1)的解 x, y, 求出使 $z \cdot x, z \cdot y$ 也是(5·1)的解的有限多个 z 没有任何困难. 因此我们可假定 $(x, y) = 1$. 令

$X = \max_{1 \leqslant i \leqslant s} \mathrm{ord}_{p_i}(x \cdot y)$

$C_1 = 2^{9 \cdot s + 26} \cdot s^{s+4} \cdot \max(1, \frac{1}{\log p_1}) \cdot [\prod_{i=2}^{s} \log p_i] \cdot \log(e \cdot \log p_{s-1})/(1 - \delta)$,

$C_2 = 2 \cdot \log 2/\log p_1 + 2 \cdot C_1 \cdot \log(e \cdot C_1 \cdot \log p_s)$.

定理 5·1 (5·1)的解满足 $X<C_2$.

证明 若 $y\leqslant\frac{1}{2}\cdot x$, 则 $y^{\delta}>x-y\geqslant y$, 这与 $y\geqslant1$ 矛盾. 所以 $y>\frac{1}{2}\cdot x$. 设 $\Lambda=\log(x/y)$. 则

$$0<\Lambda<x/y-1<y^{-(1-\delta)}<\left(\frac{1}{2}\cdot x\right)^{-(1-\delta)} \tag{5·2}$$

由 $x=\max(x,y)\geqslant p_1^X$, 得

$$0<\Lambda<2^{1-\delta}\cdot p_1^{-(1-\delta)\cdot X}. \tag{5·3}$$

对满足 $n=s, q=2$ 的 Λ 应用 Waldschmidt 的结果, 引理 2·4. 注意'独立的条件'$[Q(\sqrt{p_1},\cdots,\sqrt{p_n}):Q]=2^n$ 成立. 因为 $p_i\geqslant3$, 故 $V_i=\log p_i$ 对 $i\geqslant2$ 成立. 因此

$$\Lambda>\exp[-(\log X+\log(e\cdot\log p_s))\cdot C_1\cdot(1-\delta)\cdot\log p_1].$$

此式与(5·3)结合, 得

$$X<C_1\cdot\log(e\cdot\log p_s)+\log2/\log p_1+C_1\cdot\log X.$$

由于 $C_1>e^2$, 故由引理 2·1 便得结论.

例 对于 $s=2, 2\leqslant p_i\leqslant199, \delta=0.9$, 有 $C_1<2.30\times10^{17}$, $C_2<1.97\times10^{19}$.

对于 $s=6, 2\leqslant p_i\leqslant13, \delta=\frac{1}{2}$, 有 $C_1<8.37\times10^{33}$, $C_2<1$ 35×10^{36}.

5·3 在一维情形降低上界

本节作出例子：$s=2,\delta=0.9$，而 p_1,p_2 跑遍 200 以内的素数集合，或跑遍 50 以内的非幂集合（我们没有用到 p_i 是素数）. 我们注意到对任意其它三个一组的 p_1,p_2,δ，做法是类似的. 我们证明下面结果.

定理 5·2 (a)丢番图不等式

$$|p_1^{x_1}-p_2^{x_2}|<\min[p_1^{x_1},p_2^{x_2}]^{\delta} \tag{5·4}$$

满足素数 p_1,p_2 使得 $p_1<p_2<200$，且

$$\begin{aligned}&x_1,x_2\in Z,\ x_1\geqslant 2,\ x_2\geqslant 2,\\&\delta=\frac{1}{2}\text{ 或 }\delta=0.9,\ \min[p_1^{x_1},p_2^{x_2}]>10^{15}\end{aligned} \tag{5·5}$$

仅有 77 个解如第 5·5 节表 I 中所列.

(b) 丢番图不等式(5·4)满足非幂 p_1,p_2 使得 $2\leqslant p_1<p_2<50$ 以及条件(5·5)，仅有 74 个解如第 5·5 节中表 II 所列.

注：表 I，II 中，"delta"列给出的实数满足

$$|p_1^{x_1}-p_2^{x_2}|=\min[p_1^{x_1},p_2^{x_2}]^{\text{delta}}.$$

注意在定理 5·2 中没有要求 $(x_1,x_2)=1$，而在定理 5·2(b)中不要求 p_1,p_2 是素数. 条件(5·5)的选择使得(5·4)满足 $\delta=0.9$ 及 $\min[p_1^{x_1},p_2^{x_2}]$ 的很多解不需太多的努力便能找到.

证明 写

$$\Lambda = |x_1 \cdot \log p_1 - x_2 \cdot \log p_2|, X = \max(x_1, x_2).$$

假定

$$p_1^X > 10^{25}, \qquad (5 \cdot 6)$$

因为这容易求出留下的解. 设 $\log p_1 / \log p_2$ 有简单连分数展式（看 3·2 节）

$$\log p_1 / \log p_2 = [0, a_1, a_2, \cdots],$$

并设对 $n = 1, 2, \cdots$, 收敛于 r_n/q_n. 我们可设 $(x_1, x_2) = 1$. 首先证明 $x_1 \geqslant x_2$. 因若 $x_1 < x_2$, 则

$$\Lambda = x_2 \cdot \log p_2 - x_1 \cdot \log p_1 > X \cdot [\log p_2 - \log p_1] \geqslant X \cdot \log \frac{199}{197},$$

则从(5·3)和(5·6)导出

$$0.0101 \leqslant 0.0101 \cdot X < X \cdot \log \frac{199}{197} < \Lambda < 2^{0.1} \cdot 10^{-5/2} < 0.0034.$$

矛盾. 因此 $x_1 \geqslant x_2$, 因此 $X = x_1$. 其次证明

$$p_1^{X/10} > 3.1 \cdot X. \qquad (5 \cdot 7)$$

也就是, 假定不然, 则 $2^{X/10} \leqslant 3.1 \cdot X$, 这导出 $X \leqslant 80$. 这与 $3.1 \cdot X \geqslant p_1^{X/10} < 10^{5/2}$ 矛盾. 由(5·3)得

$$\left|\frac{x_2}{X}-\frac{\log p_1}{\log p_2}\right|<\frac{2^{0.1}}{\log p_2}\cdot p_1^{-X/10}\cdot\frac{1}{X}. \tag{5·8}$$

由(5·7)导出

$$\left|\frac{x_2}{X}-\frac{\log p_1}{\log p_2}\right|<\frac{2^{0.1}}{\log 2}\cdot\frac{1}{3.1\cdot X^2}<\frac{1}{2\cdot X^2}.$$

因此由引理 3·1, x_2/X 收敛于 $\log p_1/\log p_2$, 大约是 r_k/q_k. 从 5·2 节末尾的例我们看到 $X\leqslant X_0<1.97\times10^{19}$. 由(3·7)得 $k\leqslant 92.996$, 因此 $k\leqslant 92$. 由引理 3·1 再导出: 若(5·3)成立, 则

$$a_{k+1}>-2+p_1^{q_k/10}\cdot\frac{1}{q_k}\cdot\frac{\log p_2}{2^{0.1}}, \tag{5·9}$$

又若

$$a_{k+1}>p_1^{q_k/10}\cdot\frac{1}{q_k}\cdot\frac{\log p_2}{2^{0.1}}, \tag{5·10}$$

则(5·3)对$(x_1, x_2)=(q_k, r_k)$成立. 我们计算连分数展式并在 p_1, p_2 的论及范围内计算收敛的所有数 $\log p_1/\log p_2$ 精确到下标 n 使 $q_{n-1}\leqslant 1.97\cdot10^{19}<q_n$(见 2·5 节关于计算方法的叙述). 注意到 $n\leqslant 93$. 我们对(5·9)检验所有收敛, 随后又对(5·10)检验. 有可能, 虽然未必可能, 存在一个收敛满足(5·9)但对(5·10)失效. 我们仅遇到这样一种情形: $p_1=15$, $p_2=23$, 满足 $\log15/\log23=[0, 1, 6, 2, 1, 51, \cdots]$, 因此 $a_5=51$, $r_4=19$, $q_4=22$. 现在, (5·9)成立但(5·10)失效, 因为

$$15^{2.2}\cdot\frac{1}{22}\cdot(\log 23)/2^{0.1}=51.4\cdots\in[51,53).$$

在此情形有 $\Lambda=0.002714\cdots<0.002771\cdots=2^{0.1}\cdot15^{-22}$，因此(5·3)成立．但 $\log(15^{22}-23^{10})/\log(23^{10})=0.9008\cdots>\delta$，因此(5·1)不成立．这个例子说明了(5·3)比(5·1)弱．因此求出(5·3)所有的解正好检验了(5·1)．现在，用计算的叙述可完成证明，这里从略．

注：1．定理 5·2(a)用于定理 6·2 的证明．

2．定理 5·2 证明中的计算取 35 秒．

5·4　在多维情形降低上界

现设 $s\geq3$．令 $x_i=\mathrm{ord}_{p_i}(x/y)$，$i=1,\cdots,s$，那么 $X=\max|x_i|$，又

$$\Lambda=\sum_{i=1}^{s}x_i\cdot\log p_i.$$

注意到(5·3)属于(3·1)型．因此由定理 5·1，我们可用 3·7 节所述的方法来解(5·3)，我们以 $s=6$，$\{p_1,\cdots,p_6\}=\{2,3,5,7,11,13\}$(前 6 个素数)，以及 $\delta=\frac{1}{2}$ 为例．

我们应用引理 3·7 和 3·8，对这一应用特别设计如下．设记号如 3·7 节．

引理 5·3　设 X_1 是一个正数，使得

$$\iota(\Gamma)\geq\sqrt{4\cdot n^2+(n-1)\cdot r^2}\cdot X_1\qquad(5\cdot11)$$

则(5·3)没有满足对 $i=1,\cdots,s$，

$$\log[r\cdot C\cdot\sqrt{2}/s\cdot X_1]/\frac{1}{2}\cdot\log p_1\leqslant|x_i|\leqslant X\leqslant X_1 \quad (5\cdot12)$$

的解.

引理 5·4　假定

$$|\widetilde{\Lambda}|>\sum_{i=1}^{s}|x_i| \quad (5\cdot13)$$

则

$$|x_i|<\log[r\cdot C\cdot\sqrt{2}/[|\lambda|-\sum_{i=1}^{s}|x_i|]]/(1-\delta)\cdot\log p_i \quad (5\cdot14)$$

注:引理 5·3 和 5·4 是引理 3·8 的精确,其差异在不同的 x_i 之间.再者,引理 5·3 有着比引理 3·7 稍微明显的条件和结论.

证明(引理 5·3 和 5·4)　仿照引理 3·7 和 3·8 的证明,利用(5·2)以及

$$p_i^{|x|}\leqslant\max(x,y)=x<2\cdot|\Lambda|^{-1/2}.$$

定理 5·5　丢番图不等式

$$0<x-y<\sqrt{y}$$

其中 $x,y\in S=\{2^{x_1}\cdot\cdots\cdot13^{x_6}\ x_i\in N_0,i=1,\cdots,6\}$,满足$(x,y)=1$,恰有 605 个解.这些解中,571 个解满足

$$\mathrm{ord}_2(x\cdot y)\leqslant 19,\ \mathrm{ord}_3(x\cdot y)\leqslant 12,\ \mathrm{ord}_5(x\cdot y)\leqslant 8,$$

$$\mathrm{ord}_7(x\cdot y)\leqslant 7,\quad \mathrm{ord}_{11}(x\cdot y)\leqslant 5,\ \mathrm{ord}_{13}(x\cdot y)\leqslant 5$$

剩下的 34 个解列在第 5·5 节表册中.

注:$\mathrm{ord}_{p_i}(x\cdot y)$的上界给出的 571 个解没有列入表册中,这一选择,是要使得这种只凭着手算求出所有解的方法,在计算时间上得到适当控制.列出所有 605 个解篇幅太长,不能在这里复制.

证明　由 5·2 节末尾的例可知,当 $X_0=1.35\times10^{36}$时,$X<X_0$.我们应用 3·7 节中所述方法.取 $C=10^{240}$(如此选择,使它比 X_0^6 稍微大些),并取 $r=1$.我们将 L^3-运算应用于对应的格 Γ_1,并求出满足$|c_1|>9.40\times10^{39}$的一个简化基 $c_1,\cdots,c_6$.由引理 3·4,

$$c(\Gamma_1)>2^{-5/2}\cdot9.40\times10^{40}>1.66\times10^{39}$$

这比 $\sqrt{4.6^2+5.1^2}\cdot X_0=1.64\cdots\times10^{37}$要大些,因此(5·11)对 $X_1=X_0$ 成立.由引理 5·3,我们发现

$$X<\log[10^{240}\cdot\sqrt{2}/6\cdot1.35\times10^{36}]/\frac{1}{2}\cdot\log2$$
$$<1350.4,$$

因此 $X\leqslant1350$.其次,取 $C=10^{32}$,$r=1$,$X_0=1350$.算出对应格 Γ_2 的简化基,我们找到$|c_1|>2.71\times10^5$.因此 $c(\Gamma_2)>4.79\times10^4$,它比 $\sqrt{149}\cdot1350=1.64\cdots\times10^4$ 大.因此引理 5·3 导出对

所有 $i=1,\cdots,6$

$$|x_i| < \log[10^{32}\cdot\sqrt{2}/6\cdot 1350]/\frac{1}{2}\cdot\log p_i,$$

由此得

$$\begin{gathered}|x_1|\leqslant 187,\quad |x_2|\leqslant 118,\quad |x_3|\leqslant 80,\\ |x_4|\leqslant 66,\quad |x_5|\leqslant 54,\quad |x_6|\leqslant 50.\end{gathered} \tag{5·15}$$

其次，选择 $C=10^{12}$, $r=10^4$. 我们应用引理 5·4 如下. 若 $|\lambda|>10^6$，则由(5·15)，可知(5·13)成立，由引理 5·4 导出

$$\begin{gathered}|x_1|\leqslant 67,\quad |x_2|\leqslant 42,\quad |x_3|\leqslant 29,\\ |x_4|\leqslant 24,\quad |x_5|\leqslant 19,\quad |x_6|\leqslant 18.\end{gathered} \tag{5·16}$$

满足(5·15)和 $|\lambda|<10^6$ 的对应格 Γ_3 中所有向量已由 Fincke 和 Pohst 运算计算出来，参看 3·6 节. 我们略去阐述. 我们发现仅存在两个这样的向量，但他们不对应于(5·1)的解. 因此(5·1)所有的解满足(5·16). 接着，取 $C=10^8$, $r=10^4$. 若 $|\lambda|>5\times10^5$，则引理 5·4 导出

$$\begin{gathered}|x_1|\leqslant 42,\quad |x_2|\leqslant 27,\quad |x_3|\leqslant 18,\\ |x_4|\leqslant 15,\quad |x_5|\leqslant 12,\quad |x_6|\leqslant 11.\end{gathered} \tag{5·17}$$

对应格 Γ_3 中有 143 个向量满足(5·16)和 $|\lambda|\leqslant 5\times10^5$. 其中 2 个对应于(4·1)的解，即满足

$$(x_1, \cdots, x_6) = (7, -5, 3, -9, -3, 8), \ \lambda = 257674,$$

$$(x_1, \cdots, x_6) = (-10, 10, -6, 5, -6, 4), \ \lambda = 144817$$

这两个向量也满足(5·17).因此(5·1)所有的解满足(5·17).这方面,选择适当的参数 C, r, 以及 λ_i 的上界,对满足重复的程序似乎是无效的.但(5·17)的界小得容许列举.这样做,我们便找到结果.

注:定理 5·2 和 5·5 在解其他指数丢番图方程方面得到应用,可参见 Stroeker 和 Tijdeman[114]、Alex[3],[4], Tijdeman 和 Wang[120],郭永东[47]以及本书的 6·4 节.

注:Γ_1 的简化运算取 113 秒.其中我们应用的 L^3 运算如 3·5 节第 12 步所述.(5·17)的解的直接检验取 228 秒,剩下的运算(计算 $\log p_i$ 到 250 小数位,计算 Γ_2 的简化基及 Γ_3 和 Γ_4 中的短向量)取 8 秒.因此总数用 349 秒.

5·5 表

Table I. (Theorem 5.2(a)).

p_1	x_1	$p_1^{x_1}$	p_2	x_2	$p_2^{x_2}$	delta
2	3	8	3	2	9	0.00000
3	3	27	5	2	25	0.21534
2	5	32	3	3	27	0.48832
5	3	125	11	2	121	0.28906
2	7	128	11	2	121	0.40575
2	7	128	5	3	125	0.22754
2	8	256	3	5	243	0.46694
7	3	343	19	2	361	0.49512
2	9	512	23	2	529	0.45416
3	7	2187	13	3	2197	0.29941
3	7	2187	47	2	2209	0.40194
13	3	2197	47	2	2209	0.32293
19	3	6859	83	2	6889	0.38504
31	3	29791	173	2	29929	0.47828
2	15	32768	181	2	32761	0.18716
13	7	627 48517	89	4	627 42241	0.48703
2	50	1 12589 99068 42624	47	9	1 11913 04731 02767	0.85259
7	18	1 62841 35979 10449	149	7	1 63043 64614 03549	0.80898
19	12	2 21331 49190 66161	83	8	2 25229 22321 39041	0.88568
2	51	2 25179 98136 85248	19	12	2 21331 49190 66161	0.88532
2	51	2 25179 98136 85248	83	8	2 25229 22321 39041	0.76159
5	22	2 38418 57910 15625	157	7	2 35124 32775 37493	0.87942
13	14	3 93737 63856 99289	89	8	3 93658 88057 02081	0.76282
17	13	9 90457 80329 05937	193	7	9 97473 03260 05057	0.86560

p_1	x_1	$p_1^{x_1}$	p_2	x_2	$p_2^{x_2}$	delta
7	19	11 39889 51853 73143	197	7	11 51499 04768 98413	0.87594
61	9	11 69414 60928 34141	197	7	11 51499 04768 98413	0.88743
5	23	11 92092 89550 78125	61	9	11 68414 60928 34141	0.89343
5	23	11 92092 89550 78125	29	11	12 20050 97657 05829	0.89862
29	11	12 20050 97657 05829	199	7	12 35866 42791 61399	0.88268
23	12	21 91462 44320 20321	43	10	21 61148 23132 84249	0.88656
11	16	45 94972 98635 72161	71	9	45 84850 07184 49031	0.84059
5	24	59 60464 47753 90625	73	9	58 87158 67082 67913	0.88642
37	11	177 91762 17794 60413	53	10	174 88747 03655 13049	0.89785
29	12	353 81478 32054 69041	89	9	350 35640 37074 85209	0.88568
23	13	504 03636 19364 67383	163	8	498 31141 43181 21121	0.89040
23	13	504 03636 19364 67383	59	10	511 11675 33006 41401	0.89536
11	17	505 44702 84992 93771	163	8	498 31141 43181 21121	0.89580
11	17	505 44702 84992 93771	23	13	504 03636 19364 67383	0.85578
11	17	505 44702 84992 93771	59	10	511 11675 33006 41401	0.88985
7	21	558 54586 40832 84007	41	11	550 32903 17162 48441	0.89708
19	14	799 00668 57828 84121	31	12	787 66278 37885 49761	0.89710
19	14	799 00668 57828 84121	173	8	802 35917 84760 91681	0.86722
2	60	1152 92150 46068 46976	181	8	1151 93665 78235 00641	0.83013
67	10	1822 83780 45517 61449	107	9	1838 45921 24201 54507	0.88680
47	11	2472 15921 50840 12303	199	8	2459 37419 15531 18401	0.87580
13	17	8650 41591 93813 37933	127	9	8594 75474 86093 97887	0.88441
2	63	9223 37203 68547 75808	53	11	9269 03592 93721 91597	0.87844
3	41	36472 99637 71707 86403	149	9	36197 31987 96201 91349	0.89170
2	65	36893 48814 74191 03232	5	28	37252 90298 46191 40625	0.89721
2	66	73786 97629 48382 06464	97	10	73742 41268 94928 26049	0.83799

p_1	x_1	$p_1^{x_1}$	p_2	x_2	$p_2^{x_2}$	delta
3	42	1 09418 98913 15123 59209	101	10	1 10462 21254 11204 51001	0.89916
2	68	2 95147 90517 93528 25856	29	14	2 97558 23267 57994 63481	0.89800
113	10	3 39456 73899 22223 14849	191	9	3 38298 68155 95733 17311	0.87990
53	12	4 91258 90425 67261 54641	199	9	4 89415 46411 90705 61799	0.88284
5	30	9 31322 57461 54785 15625	41	13	9 25103 10231 50136 29321	0.89638
19	17	54 80386 85778 48021 85939	47	13	54 60999 70612 05831 77327	0.88730
23	16	61 32610 41568 09986 48961	151	10	61 62677 95033 67185 14001	0.89400
2	73	94 44732 96573 92904 27392	7	26	93 87480 33764 77543 05649	0.89920
2	75	377 78931 86295 71617 09568	181	10	377 38596 84695 57044 99801	0.86840
2	75	377 78931 86295 71617 09568	41	14	379 29227 19491 55588 02161	0.89368
41	14	379 29227 19491 55588 02161	181	10	377 38596 84695 57044 99801	0.89828
3	49	2392 99329 23061 75295 90083	17	19	2390 72435 68515 13248 47153	0.87071
13	21	2470 64529 07345 03927 04413	89	12	2469 90403 56526 21403 03521	0.84941
103	12	14257 60886 84617 89454 47841	157	11	14285 52404 46318 60195 25093	0.88788
3	51	21536 93963 07555 77663 10747	163	11	21580 60662 62396 00904 07387	0.88933
7	29	32199 05755 81317 97268 37607	13	22	32118 38877 95485 51051 57369	0.89390
11	24	98497 32675 80761 10947 11841	61	14	98768 32533 36131 80951 12441	0.89755
37	16	1 23375 11914 21716 63622 74241	191	11	1 23414 74201 97479 41888 22591	0.86078
2	84	1 93428 13113 83406 67952 98816	199	11	1 93813 41794 57931 33178 02199	0.89319
2	84	1 93428 13113 83406 67952 98816	193	53	1 93832 45667 68001 98967 96723	0.89402
3	53	1 93832 45667 68001 98967 96723	199	11	1 93813 41794 57931 33178 02199	0.84151
7	30	2 25393 40290 69225 80878 63249	31	17	2 25501 16774 16274 31786 82911	0.86903
2	90	123 79400 39285 38027 48991 24224	181	12	123 63541 71303 11583 51179 80561	0.89326
43	17	587 44031 06360 42001 88795 53643	71	15	587 32059 59385 49335 38673 30551	0.86709
2	99	63382 53001 14114 70074 83516 02688	97	15	63325 11891 36789 38604 32759 54593	0.89791
2	102	5 07060 24009 12917 60598 68128 21504	83	16	5 07282 02989 53863 75247 83563 99681	0.89060
13	28	15 50293 28026 62396 21526 95351 05521	89	16	15 49673 14251 78936 43509 93277 30561	0.89106

Table II. (Theorem 5.2(b)).

p_1	x_1	$p_1^{x_1}$	p_2	x_2	$p_2^{x_2}$	delta
2	3	8	3	2	9	0.00000
3	3	27	5	2	25	0.21534
2	5	32	3	3	27	0.48832
2	5	32	6	2	36	0.40000
5	3	125	11	2	121	0.28906
2	7	128	11	2	121	0.40575
2	7	128	5	3	125	0.22754
6	3	216	15	2	225	0.40876
2	8	256	3	5	243	0.46694
7	3	343	19	2	361	0.49512
2	9	512	23	2	529	0.45416
2	10	1024	10	3	1000	0.46007
6	4	1296	11	3	1331	0.49607
12	3	1728	42	2	1764	0.48070
2	11	2048	45	2	2025	0.41184
3	7	2187	13	3	2197	0.29941
3	7	2187	47	2	2209	0.40194
13	3	2197	47	2	2209	0.32293
15	4	50625	37	3	50653	0.30762
6	7	2 79936	23	4	2 79841	0.36309
2	50	1 12589 99068 42624	47	9	1 11913 04731 02767	0.85259
2	50	1 12589 99068 42624	18	12	1 15683 13814 26176	0.89628
24	11	1 52168 11431 69024	33	10	1 53157 89852 64449	0.85597
15	13	1 94619 50683 59375	50	9	1 95312 50000 00000	0.83986
2	51	2 25179 98136 85248	19	12	2 21331 49190 66161	0.88532
6	20	3 65615 84400 62976	26	11	3 67034 44869 87776	0.84507

p_1	x_1	$p_1^{x_1}$	p_2	x_2	$p_2^{x_2}$	delta
11	15	4 17724 81694 15651	20	12	4 09600 00000 00000	0.89095
28	11	8 29350 94674 71872	39	10	8 14040 60851 91601	0.89154
10	16	10 00000 00000 00000	17	13	9 90457 80329 05937	0.87396
5	23	11 92092 89550 78125	29	11	12 20050 97657 05829	0.89862
2	54	18 01439 85094 81984	30	11	17 71470 00000 00000	0.89096
23	12	21 91462 44320 20321	43	10	21 61148 23132 84249	0.88656
6	21	21 93695 06403 77856	23	12	21 91462 44320 20321	0.81690
6	21	21 93695 06403 77856	43	10	21 61148 23132 84249	0.88845
2	55	36 02879 70189 63968	24	12	36 52034 74360 56576	0.88735
19	13	42 05298 34622 57059	46	10	42 42074 74827 76576	0.87619
3	35	50 03154 50989 99707	33	11	50 54210 65137 26817	0.88076
13	15	51 18589 30140 90757	33	11	50 54210 65137 26817	0.88656
26	12	95 42895 66616 82176	35	11	96 54915 73730 46875	0.88631
35	11	96 54915 73730 46875	50	10	97 65625 00000 00000	0.88575
14	15	155 56809 55578 12224	21	13	154 47237 77391 19461	0.87497
11	17	505 44702 84992 93771	23	13	504 03636 19364 67383	0.85578
7	21	558 54586 40832 84007	41	11	550 32903 17162 48441	0.89708
6	23	789 73022 30536 02816	31	12	787 66278 37885 49761	0.85579
6	23	789 73022 30536 02816	19	14	799 00668 57828 84121	0.89216
19	14	799 00668 57828 84121	31	12	787 66278 37885 49761	0.89710
26	13	2481 15287 32037 36576	47	11	2472 15921 50840 12303	0.86739
28	13	6502 11142 24979 47648	37	12	6582 95200 58400 35281	0.89872
15	16	6568 40835 57128 90625	28	13	6502 11142 24979 47648	0.89414
15	16	6568 40835 57128 90625	37	12	6582 95200 58400 35281	0.85892
2	65	36893 48814 74191 03232	5	28	37252 90298 46191 40625	0.89721
37	13	2 43569 22421 60813 05397	50	12	2 44140 62500 00000 00000	0.87101

p_1	x_1	$p_1^{x_1}$	p_2	x_2	$p_2^{x_2}$	delta
2	68	2 95147 90517 93528 25856	29	14	2 97558 23267 57994 63481	0.89800
11	20	6 72749 99493 25600 09201	40	13	6 71088 64000 00000 00000	0.87486
5	30	9 31322 57461 54785 15625	41	13	9 25103 10231 50136 29321	0.89638
35	14	41 39545 12236 93847 65625	46	13	41 29065 87698 35408 01536	0.87993
19	17	54 80386 85778 48021 85939	47	13	54 60990 70612 05831 77327	0.88730
6	28	61 40942 21446 48154 97216	23	16	61 32610 41568 09986 48961	0.86842
2	73	94 44732 96573 92904 27392	7	26	93 87480 33764 77543 05649	0.89920
20	17	131 07200 00000 00000 00000	38	14	130 90925 53986 67734 38464	0.86863
2	74	188 89465 93147 85808 54784	39	14	188 32349 19413 17426 09041	0.88695
2	75	377 78931 86295 71617 09568	41	14	379 29227 19491 55588 02161	0.89368
3	49	2392 99329 23061 75295 90083	17	19	2390 72435 68515 13248 47153	0.87071
15	20	3325 25673 00796 50878 90625	37	15	3334 46267 95181 53070 88493	0.89126
19	19	19784 19655 66031 35891 23979	33	16	19779 85201 46255 88779 34081	0.84943
7	29	32199 05755 81317 97268 37607	13	22	32118 38877 95485 51051 57369	0.89390
2	84	1 93428 13113 83406 67952 98816	3	53	1 93832 45667 68001 98967 96723	0.89402
7	30	2 25393 40290 69225 80878 63249	31	17	2 25501 16774 16274 31786 82911	0.86903
11	25	10 83470 59433 88372 20418 30251	34	17	10 84280 35605 96593 23542 07744	0.87991
14	23	22 95856 92886 98149 54822 20544	18	2[illegible]	22 94682 51895 12940 71398 72768	0.87516
23	20	171 61558 31334 58634 29238 95201	40	17	171 79869 18400 00000 00000 00000	0.89088
6	35	171 90707 99748 42259 10286 58176	23	20	171 61558 31334 58634 29238 95201	0.89829
6	35	171 90707 99748 42259 10286 58176	40	17	171 79869 18400 00000 00000 00000	0.88250
15	25	25251 16829 40423 48861 69433 59375	43	18	25259 93335 73498 06081 18208 06649	0.88234

Table III. (Theorem 5.5)

x_1	x_2	x_3	x_4	x_5	x_6	x	y	x − y
−1	−11	−1	0	6	0	17 71561	17 71470	91
0	4	5	1	−6	0	17 71875	17 71561	314
21	−2	−2	−1	−3	0	20 97152	20 96325	827
1	13	−1	−3	−1	−2	31 88646	31 88185	461
19	0	0	−8	1	0	57 67168	57 64801	2367
6	2	−1	1	6	3	88 58304	88 57805	499
2	15	−1	−2	−4	0	143 48907	143 48180	727
11	−15	0	2	1	1	143 50336	143 48907	1429
1	8	−1	−8	0	3	288 29034	288 24005	5029
22	5	1	−1	1	3	293 62905	293 60128	2777
13	1	3	−1	1	−6	337 92000	337 87663	4337
1	2	9	−4	−4	0	351 56250	351 53041	3209
3	3	0	4	2	−7	627 52536	627 48517	4019
26	1	0	5	3	0	671 10351	671 08864	1487
3	−13	10	−2	0	0	781 25000	781 21827	3173
8	−2	−10	4	1	1	878 95808	878 90625	5183
25	1	−4	0	−5	0	1006 63296	1006 56875	6421
6	1	2	−6	0	7	1882 45551	1882 38400	7151
8	−13	0	3	2	3	1929 14176	1929 13083	1093
1	13	−3	7	2	0	1992 97406	1992 90375	7031
4	−1	4	1	−4	7	4392 39619	4392 30000	9619
4	2	−11	2	6	0	7812 58401	7812 50000	8401
16	−3	5	1	1	−6	14336 0000	14335 62273	37727
8	8	0	−8	3	2	14758 24779	14757 89056	35723
5	−2	−5	11	0	−3	19773 26743	19773 00000	26743
25	7	1	0	−2	5	40600 88955	40600 86272	2683
2	0	13	−9	−2	0	48828 12500	48827 86447	26053
−14	19	−2	−4	1	−1	1 27848 76137	1 27848 44800	31337
−24	−1	−2	12	−1	0	1 38412 87201	1 38412 03200	84001
−5	5	10	0	1	−8	2 61035 15625	2 61033 83072	1 32553
2	−4	−9	3	7	−2	2 67363 98612	2 67363 28125	70487
18	7	0	−13	0	2	9 68892 08832	9 68890 10407	1 98425
7	−5	3	−9	−3	8	1305 16915 36000	1305 16881 72831	33 63169
−10	10	−6	5	−6	4	2834 49801 04623	2834 49760 00000	41 04623

第六章　S－整数方程 $x+y=z$

6.1 导言

设 S 是由固定有限集 $\{p_1, \cdots, p_s\}$ 中的素数组成的所有正整数集合，其中 $s \geqslant 3$. 本章致力于丢番图方程

$$x+y=z \tag{6.1}$$

其中 $x, y, z \in S$. 不失一般性，可设 x, y, z 是不同素数. 对任意 $a \in S$，我们定义

$$m(a) = \max_{1 \leqslant i \leqslant s} \operatorname{ord}_{p_i}(a).$$

Mahler[73]已证明(6.1)仅有有限多个解，但他的证明是无效的. 有效的说法，即：关于(6.1)的解 x, y, z 的 $m(x \cdot y \cdot z)$ 的有效可计算上界可以由 Coates[32]，[33]和 Sprindžuk[108]的结果导出，因为(6.1)可简化成有限多个 Thue 方程. 也可参考 Shorey 和 Tijdeman[107]第一章.

在 6.2 节我们导出一个显示上界. 6.3 节专用于 p－adic 逼近格的详述，6.4 和 6.5 节的简化方法建立在这上面. 在 6.4 节我们给出(6.1)在一维情形 $s=3$ 的一种解法. 这种解法基于在 3.10 节中给出的简化程序，我们也结合用与 4.8 节类似的 p－adic 和实的逼近技术，但我们现在可将实际进行的实简化步骤简单地归于第五章的结果. 作为一个例子，我们求出稍微一般的方程 $x \pm y = w \cdot z$ 的全部解，其中 x, y, z 是 2、3、

5 的解，$w \in Z$，$|w| \leq 1000000$，$(w, z) = 1$.

在 6.5 节，给出解(6.1)在多维情形 $s \geq 4$ 的一个程序，它建立于 3.11 节所述的简化程序上. 我们作出例子$\{p_1, \cdots, p_6\} = \{2, 3, 5, 7, 11, 13\}$，并实际确定其全部解. 这推广了 Alex [2]的结果，Alex 用初等观点对$\{p_1, \cdots, p_4\} = \{2, 3, 5, 7\}$的情形给出(6.1)的完满解答. 也参见 Rumsey 和 Posner[100]以及 Brenner 和 Foster[23]. 在 6.6 节，我们用与方程(6.1)有关的 Oesterlé - Masser 猜想及熟知的"abc" - 猜想的注释作为结束. 实际上，我们解(6.1)的方法导出了发现有关 abd - 猜想有趣例子的方法. 最后，在 6.7 节给出表格.

6.2 上界

本节给出(6.1)解的一个上界，这建立在引理 2.6 上(参考于坤瑞[141]). 注意 de Weger[136]使用的结果代替了 Van der Poorten[98](也看 de Weger[136]的修改).

我们引入一些记号. 假定 $p_1 < \cdots < p_s$. 设 q_i 是满足 $q_i \nmid p_i(p_i - 1)$，$i = 1, \cdots, s$ 的最小素数. 令

$$t = [2 \cdot s/3],\quad p = \prod_{i=1}^{s} p_i,\quad q = \max_i q_i,$$

$C_1(2, t)$和 a_1 如引理 2.6，满足 $n = t$.

$$U = C_1(2, t) \cdot a_1^t \cdot t^{t+5/2} \cdot q^{2t} \cdot (q - 1) \cdot \log^2(t \cdot q) \cdot \max_i$$

$$\frac{(p_i-1)\cdot[2+\frac{1}{p_i-1}]^t}{(\log p_i)^{t+2}}\cdot(\log p_s)^t\cdot[\log(4\cdot\log p_s)+\frac{\log p_s}{8\cdot t}],$$

$$C_1=U/6\cdot t,\quad C_2=U\cdot\log 4,$$

$$V_i=\max(1,\log p_i)^t,\ i=s-t+1,\cdots,s,\ \Omega=\prod_{i=s-t+1}^{s}V_i,$$

$$C_3=2^{9\cdot t+26}\cdot t^{t+4}\cdot\Omega\cdot\log(e\cdot V_{s-1}),$$

$$C_4=\max[7.4,[C_1\cdot\log(p/p_1)+C_3]/\log p_1],$$

$$C_5=[C_2\cdot\log(p/p_1)+C_3\cdot\log(e\cdot V_s)+0.327]/\log p_1,$$

$$C_6=\max[C_5,(C_2\cdot\log(p/p_1)+\log 2)/\log p_1],$$

$$C_7=2\cdot[C_6+C_4\cdot\log C_4],$$

$$C_8=\max[p_s,\log[2\cdot(p/p_1)^{p_s}]/\log p_1,C_2+C_1\cdot\log C_7,C_7].$$

现在我们阐明主要结果.

定理 6.1　(6.1)的解满足 $m(x\cdot y\cdot z)\leqslant C_8$.

证明　若我们考虑(6.1)的等价方程

$$x\pm y=z \tag{6.2}$$

则我们可假定 $x\cdot y$ 至多有 t 个素因子 $p_{i_1},\cdots,p_{i_t}$.

比如.首先假定 $m(x\cdot y)\leqslant p_s$,则

$$p_1^{m(z)}\leqslant z\leqslant 2\cdot\max(x,y)<2\cdot(p/p_1)^{p_s},$$

因此

$$m(x\cdot y\cdot z)<\max[p_s,\log[2\cdot(p/p_1)^{p_s}]/\log p_1]\leqslant C_8.$$

其次假定 $m(x\cdot y)\geqslant p_s$ 且 $m(z)\geqslant 2$.则对某 $p=p_i$.

$$m(z)=\mathrm{ord}_p(z)=\mathrm{ord}_p[\pm\frac{x}{y}-1]=\mathrm{ord}_p[\log_p(\frac{x}{y})].$$

令 $x/y=\prod_{j=1}^{t}p_{i_j}^{x_{i_j}}$. 则 $m(x\cdot y)=\max_{1\leqslant j\leqslant t}|x_{i_j}|$. 我们对 $n=t, B_0=B_n=B'=B=m(x\cdot y)$应用引理 2.6(于坤瑞的引理). 因为 $m(x\cdot y)\geqslant p_s$ 且 $t\geqslant 2$, 我们有

$$W=\max[\log(1+\frac{3}{4\cdot t}\cdot B),\log B,\log p]=\log B.$$

注意对 $p=2, C_1(p,n)$取最大值. 我们得

$$m(z)<C_1\cdot\log m(x\cdot y)+C_2. \tag{6.3}$$

若 $m(z)<2$, 则(6.3)显然正确. 若(6.2)中正号成立, 则

$$(p/p_1)^{m(z)}\geqslant z>\max(x,y)\geqslant p_1^{m(x\cdot y)}.$$

由(6.3)及 $C_3>0$, 则导出

$$m(x\cdot y)<C_4\cdot\log m(x\cdot y)+C_6. \tag{6.4}$$

其次假定(6.2)中取负号. 则对此情形, 我们应用引理 2.4 来证明(6.4), 如下述. 假定(6.4)是谬误的, 则

$$\left|\frac{y}{x}-1\right|=\frac{z}{x}=\frac{z}{\max(x,y)}\leqslant\frac{(p/p_1)^{m(z)}}{p_1^{m(x\cdot y)}}<\frac{(p/p_1)^{C_1\cdot\log m(x\cdot y)+C_2}}{p_1^{C_4\cdot\log m(x\cdot y)+C_6}},$$

其值比 $\frac{1}{2}$ 小, 由 C_4 和 C_6 的规定. 因此

$$|\log\frac{y}{x}|<(2\cdot\log 2)\cdot|\frac{y}{x}-1|<(2\cdot\log 2)\cdot\frac{(p/p_1)^{C_1\cdot\log m(x\cdot y)+C_2}}{p_1^{m(x\cdot y)}}$$

另一方面，引理 2.4 导出

$$\left|\log\frac{y}{x}\right|>\exp[-C_3\cdot(\log m(x\cdot y)+\log(e\cdot V_s))].$$

因此得

$$\begin{aligned}m(x\cdot y)\cdot\log p_1&<\log(2\cdot\log 2)+(C_1\cdot\log m(x\cdot y)+C_2)\cdot\log(p/p_1)\\&\quad+C_3\cdot(\log m(x\cdot y)+\log(e\cdot V_s))\\&\leqslant(\log p_1)\cdot(C_4\cdot\log m(x\cdot y)+C_6).\end{aligned}$$

这与我们假定(6.4)是谬误的相矛盾．因而(6.4)在所有情形都成立．现在，由 $C_4>e^2$，引理 2.1 导出 $m(x\cdot y)<C_4$，而(6.3)则导出 $m(x\cdot y\cdot z)<C_8$．

例　若 $s=3$，$\{p_1,p_2,p_3\}=\{2,3,5\}$，则 $C_8<3.98\cdot10^{17}$．若 $s=6$，$\{p_1,\cdots,p_6\}=\{2,3,5,7,11,13\}$，则 $C_8<5.60\cdot10^{27}$．

6.3　p－adic 逼近格

同定理 6.1 的证明一样，我们考虑(6.2)代替(6.1)．设 p 是 $p_1,\cdots,p_s$ 中任一个素数．我们可假定 $p\nmid x\cdot y$．给其他素数重新命名如 $p_0,\cdots,p_{s-2}$，使得 $\mathrm{ord}_p(\log_p(p_0))$ 最小．对 $i=1,\cdots,s-2$，令(参看 3.11 节)

$$\theta_i = -\log_p(p_i)\log_p(p_0) = \sum_{t=0}^{\infty} u_{i,t} \cdot p^t,$$

其中 $u_{i,t} \in \{0, 1, \cdots, p-1\}$. θ_i 代替 3.11 节中的 θ'_i. 那么, 由 3.11 节明显看出如何定义关于 $\mu \in N_0$ 的 p－adic 逼近格 Γ_μ. 令

$$\Lambda = \sum_{i=1}^{s-2} x_i \cdot \theta_i - x_0.$$

则引理 3.13 导出.

$$\Gamma_\mu = \{(x_1, \cdots, x_{s-2}, x_0) \mid |\Lambda|_p \leqslant p^{-\mu}\} =$$

$$= \{(x_1, \cdots, x_{s-2}, x_0) \mid |\log_p[\prod_{i=0}^{s-2} p_i^{x_i}]|_p \leqslant p^{-(\mu+\mu_0)}\},$$

其中 $\mu_0 = \mathrm{ord}_p(\log_p(p_0))$. 在 3.13 节我们研究集

$$\Gamma_\mu^* = \{(x_1, \cdots, x_{s-2}, x_0) \mid |\prod_{i=1}^{s-2} p_i^{x_i} \pm 1|_p \leqslant p^{-(\mu+\mu_0)}\},$$

它是 Γ_μ 的一个子格. 在引理 3.17 我们说明了如何从 Γ_μ 的基求出 Γ_μ^* 的基. 实际上这很容易, 特别当 $p \geqslant 5$ 时, 就有可能选择 p_0 使得不仅 $\mathrm{ord}_p(\log_p(p_0))$ 是最小值, 而且 p_0 也是一个原根$(\mathrm{mod}\, p)$. 那么, 使用引理 3.17 的符号(满足 $\underline{b}_0$ 是基的末个元素), 选择 $\zeta = p_0 (\mathrm{mod}\, p)$, 则 $k(\underline{b}_0) = 1$, 这导出: 对于 $i = 1, \cdots, s-2$, $\underline{b}'_i = \underline{b}_i$. 由 $\underline{b}_i = [0, \cdots, 1, \cdots, 0, \theta_i^{(\mu)}]^T$, 我们有

$$p_i \cdot p_0^{\theta_i^{(\mu)}} \equiv \zeta^{k(\underline{b}_i)} (\bmod p^{\mu+\mu_0}).$$

若 $p_i \equiv p_0^{\alpha_i} (\bmod p)$，则导出

$$\gamma_i^* \equiv \alpha_i + \theta_i^{(\mu)} \equiv \alpha_i + \sum_{\iota=0}^{\mu-1} u_{i,\iota} (\bmod (p-1)/2), i = 1, \cdots, s-2,$$

$$\gamma_0^* = (p-1)/2.$$

由引理 3.14（满足 $c_1 = 0, c_2 = 1$）导出：若

$$\iota(\Gamma_\mu^*) > \sqrt{(s-1)} \cdot X_1 \tag{6.5}$$

则(6.2)没有满足

$$\mu + \mu_0 \leqslant \mathrm{ord}_p(z) \leqslant m(x \cdot y \cdot z) \leqslant X_1 \tag{6.6}$$

的解.

6.4 在一维情形降低上界

在 3.10 节我们已叙述怎样能降低(6.1)在情形 $s = 3$ 时解的上界.本节将此方法应用于下面的问题.

定理 6.2 丢番图方程

$$x \pm y = w \cdot z \tag{6.7}$$

其中 $x = p_0^{X_0}, y = p_1^{X_1}, z = p^u, (p, p_0, p_1) = (2,3,5), (3,2,5), (5,2,3), X_0, X_1, u \in N_0, w \in Z, |w| \leqslant 10^6, p \nmid w$, 对 $p = 2$ 恰有

291 个解，对 $p=3$ 恰有 412 个解，对 $p=5$ 恰有 570 个解. 满足 $u\leqslant 2$ 的全部解在第 6.7 节表 I 中列出. $u\leqslant 2$ 时的解满足：对 $p=2$, $X_0\leqslant 14$, $X_1\leqslant 9$；对 $p=3$, $X_0\leqslant 23$, $X_1\leqslant 10$, 而对 $p=5$, $X_0\leqslant 25$, $X_1\leqslant 15$.

注：(6.7)满足 $u\leqslant 2$ 的全部解容易求出. 图表在第 6.7 节中示出.

证明　设 $X=\max\limits_{p=2,3,5}\operatorname{ord}_p(x\cdot y\cdot z)$. 6.2 节末尾的例表明在 $|w|=1$ 的情形，我们有 $X<3.98\times 10^{17}$. 根据定理 6.1 不难检验对(6.7)的解也有 $X<X_0=3.98\times 10^{17}$ 成立. 令

$$x/y=p_0^{Y_0}\cdot p_1^{Y_1},\ \theta=-\log_p(p_1)/\log_p(p_0).$$

注意 θ 是 p-adic 整数. 定义格 Γ_μ, Γ_μ^* 如 6.3 节，这样，Γ_μ 由

$$\underline{b}_1=\begin{bmatrix}1\\ \theta^{(\mu)}\end{bmatrix},\quad \underline{b}_0=\begin{bmatrix}0\\ p^{\mu}\end{bmatrix}$$

生成. 对 $p=2,3$, 有 $\Gamma_\mu^*=\Gamma_\mu$, 而对 $p=5$, Γ_μ^* 的基是

$$\underline{b}_1^*=\underline{b}_1-\gamma\cdot\underline{b}_0,\quad \underline{b}_0^*=2\cdot\underline{b}_0,$$

其中，若 $\theta^{(\mu)}$ 是奇数时，$\gamma=0$, 当 $\theta^{(\mu)}$ 是偶数时，$\gamma=1$. 运用 3.10 节中给出的运算，图表 3，我们可计算 Γ_μ^* 的基 $\underline{c}_1$, $\underline{c}_2$, 这在 $|\underline{c}_1|=\iota(\Gamma_\mu^*)$ 的意义下是简化. 这样，连同 μ 在内，如下表.

p	p_0	p_1	μ_0	μ	γ	$\lvert\underline{c}_1\rvert>$	$u\leqslant$	w	$\lvert Y_0\rvert\leqslant$	$\lvert Y_1\rvert\leqslant$
2	3	5	2	143	–	2.68×10^{21}	144	$10^6\cdot 2^{144}$	114	78
3	2	5	1	91	–	2.32×10^{21}	91	$10^6\cdot 3^{91}$	182	78
5	2	3	1	65	0	5.28×10^{22}	65	$10^6\cdot 5^{65}$	189	119

$v^{(p)}$的值可在第 6.7 节表Ⅲ中找到.作为例外,我们给出下面 Γ_μ^* 的简化基(基于 p 记法):

$p=2$:

$$\underline{c}_1=\left[\begin{array}{r} 10\ 00000\ 00100\ 10001\ 10110\ 01110\ 01101 \\ 0001\ 11101\ 00101\ 00100\ 11100\ 01111\ 11010\ 00011 \\ -1\ 00010\ 00110\ 01000\ 01011\ 01110\ 00010 \\ 00111\ 00001\ 10101\ 00110\ 10011\ 00111\ 00101\ 10101 \end{array}\right]$$

$$\underline{c}_2=\left[\begin{array}{r} 10\ 11011\ 10000\ 01011\ 01101\ 11000\ 00111 \\ 11001\ 10100\ 11011\ 00000\ 11111\ 10110\ 10110\ 00001 \\ 10\ 01110\ 11101\ 10111\ 11000\ 00100\ 10101 \\ 00111\ 00001\ 10101\ 00110\ 10011\ 00111\ 00101\ 10101 \end{array}\right]$$

$p=3$:

$$\underline{c}_1=\left(\begin{array}{l} -102\ 01121\ 02221\ 00210\ 12120\ 20020\ 22222\ 10212\ 20222 \\ 21002\ 00122\ 21100\ 11102\ 22102\ 20001\ 11222\ 02212\ 21011 \end{array}\right),$$

$$\underline{c}_2=\left(\begin{array}{l} -10\ 12210\ 12111\ 01102\ 02010\ 12112\ 12210\ 21122\ 21011\ 20102 \\ -2\ \ 22021\ 11012\ 01000\ 12021\ 00211\ 12221\ 22121\ 21220\ 12122 \end{array}\right)$$

$p=5$:

$$\underline{c}_1=\left(\begin{array}{r} -211\ 32230\ 21042\ 22023\ 30141\ 33034\ 21420 \\ -22104\ 43102\ 43111\ 03114\ 30134\ 23410 \end{array}\right)$$

$$\underline{c}_2=\left(\begin{array}{l} 340\ 34003\ 02404\ 12120\ 03412\ 22030\ 32211 \\ -414\ 20001\ 42202\ 42210\ 34043\ 20120\ 00432 \end{array}\right)$$

由此,我们找到上面给出的$|\underline{c}_1|$的下界.这些下界全部比$\sqrt{2}\cdot 3.98\times 10^{17}$大.因此(6.5)对 $X_1=X_0$ 成立,则由(6.6)推断出 $u\leqslant\mu+\mu_0-1$,而$|w|\cdot z\leqslant W$ 如上表所示.现在我们寻找$|Y_0|$,$|Y_1|$的新上界如下.若在(6.7)中取负号,假定 $\min(x,y)>W^{10/9}$,我们推出

$$|x-y|=|w|\cdot z\leqslant W<\min(x,y)^{0.9}.$$

因为 $W>10^{40}$,由定理 5.2(a),不等式 $|x-y|<\min(x,y)^{0.9}$

没有满足 $\min(x,y)>W$ 的解. 因此 $\min(x,y)\leqslant W^{10/9}$, 从而

$$\max(x,y)\leqslant\min(x,y)+|w|\cdot z\leqslant W^{10/9}+W.$$

若在(6.7)中取正号, 则此不等式立即可导出. 因此上表给出的关于 $|Y_0|$, $|Y_1|$ 的界由

$$|Y_i|\cdot\log p_i\leqslant\log\max(x,y)\leqslant\log(W^{10/9}+W)$$

导出. 我们重复此程序, 连同 μ 在内列下表.

p	μ	γ	$\lvert \underset{\sim}{c}_1\rvert >$	$\sqrt{2}\cdot X_0<$	$u\leqslant$	W	$\lvert Y_0\rvert\leqslant$	$\lvert Y_1\rvert\leqslant$
2	16	–	167.7	161.3	17	$10^6\cdot 2^{17}$	34	21
3	13	–	535.8	257.4	13	$10^6\cdot 3^{13}$	49	21
5	7	1	276.1	267.3	7	$10^6\cdot 5^7$	49	31

现在, 数字小得能用手工完成计算. 例如, 对 $p=5$, 格 Γ_7^* 由

$$\underset{\sim}{b}_1^*=\begin{bmatrix}1\\-45607\end{bmatrix},\quad \underset{\sim}{b}_0^*=\begin{bmatrix}0\\156250\end{bmatrix},$$

生成. 而一个简化基是

$$\underset{\sim}{c}_1=\begin{bmatrix}185\\205\end{bmatrix},\quad \underset{\sim}{c}_0=\begin{bmatrix}-394\\408\end{bmatrix}.$$

我们找出如上表给出的关于 u 和 W 的上界. 在所有三种情形下, $W^{10/9}<10^{15}$. 假定 $\min(x,y)>10^{15}$, 我们推断出

$$|x-y|=|w|\cdot x\leqslant W<10^{15\cdot 0.9}\leqslant\min(x,y)^{0.9}.$$

由定理 5.2(a)看出, 不等式 $|x-y|<\min(x,y)^{0.9}$ 仅有两个解: $(x,y)=(2^{65},5^{28}),(2^{84},3^{53})$. 然而, 此两解都使 $|x-y|>$

$10^{15 \cdot 0.9}$. 所以我们推出 $\min(x, y) \leqslant 10^{15}$, 因此由 $\max(x, y) \leqslant 10^{15} + W$, 得到上面给出的关于 $|Y_0|$, $|Y_1|$ 的界. 这些界小得足以使剩下的情形容许列举.

注: 计算机对上述证明的计算小于 1 秒.

6.5 在多维情形降低上界

在 3.11 节已叙述怎样来降低(6.1)在 $s \geqslant 3$ 时解的上界. 在本节, 将应用此方法于下面问题.

定理 6.3 丢番图方程

$$x + y = z, \tag{6.8}$$

$x, y, z \in S = \{2^{x_1} \cdots 13^{x_6} \mid x_i \in \mathbb{N}_0, i = 1, \cdots, 6\}$, $(x, y) = 1$, $x \leqslant y$, 恰有 545 个解. 其中, 514 个解满足

$$\begin{aligned} &\mathrm{ord}_2(x \cdot y \cdot z) \leqslant 12, \quad \mathrm{ord}_3(x \cdot y \cdot z) \leqslant 7, \\ &\mathrm{ord}_5(x \cdot y \cdot z) \leqslant 5, \quad \mathrm{ord}_7(x \cdot y \cdot z) \leqslant 4, \\ &\mathrm{ord}_{11}(x \cdot y \cdot z) \leqslant 3, \quad \mathrm{ord}_{13}(x \cdot y \cdot z) \leqslant 3, \end{aligned}$$

剩下的 31 个解在第 6.7 节表 II 中给出.

注: 由定理 6.3 容易计算(6.8)所有 545 个解.

证明 从 6.2 节末尾的例我们已看到 $m(x \cdot y \cdot z) < X_0 = 5.60 \times 10^{27}$. 用 6.3 节的记号, 我们选择下面参数.

p	p_0	p_1	p_2	p_3	p_4	μ_0	μ	γ_0^*	γ_1^*	γ_2^*	γ_3^*	γ_4^*
2	3	5	7	11	13	2	605	-	-	-	-	-
3	2	5	7	11	13	1	385	-	-	-	-	-
5	2	3	7	11	13	1	275	2	0	1	1	1
7	3	2	5	11	13	1	220	3	0	-1	-1	0
11	2	3	5	7	13	1	165	5	2	0	-1	-1
13	2	3	5	7	11	1	165	6	-2	-1	-2	3

我们用 L^3 – 运算对 i = 1,2,3,4 计算 $\theta^{(\mu)}$的六个值(并在表Ⅲ中给出)以及六个格 Γ_μ^* 的简化基. 由此得到 $\iota(\Gamma_\mu^*)$的下界如下表. 他们都比$\sqrt{5}\cdot 5.60\times10^{27}$大(注意这里有很大的幅度, 我们取 μ 的值很可能大约比 20%更小). 这样我们对 $X_1 = X_0 = 5.60\times10^{27}$应用引理 3.14. 对每个 p, 我们因此得 $\mathrm{ord}_p(z)\leqslant\mu+\mu_0-1$. 由于 x, y, z 置换之下(6.2)是不变式, 我们甚至有 $\mathrm{ord}_p(x\cdot y\cdot z)\leqslant\mu+\mu_0-1$, 如下表所示.

p	$\iota(\Gamma_\mu^*\geqslant\lvert \underline{c}_1\rvert/4>$	$\mathrm{ord}_o(x\cdot y\cdot z)\leqslant$
2	4.70×10^{35}	606
3	1.15×10^{36}	385
5	6.27×10^{37}	275
7	3.17×10^{36}	220
11	5.74×10^{33}	165
13	1.73×10^{36}	165

因此, $m(x\cdot y\cdot z)\leqslant 606$.

我们对 $X_0 = 606$ 及 μ 重复步骤如下表. 在计算 6 个格 Γ_μ^*

的简化基之后我们找到下面数据. 注意在所有情形都有 $\iota(\Gamma_\mu^*)>\sqrt{5}\cdot 606$.

p	μ	γ_0^*	γ_1^*	γ_2^*	γ_3^*	γ_4^*	$\iota(\Gamma_\mu^*)>$	$ord_p(x\cdot y\cdot z)\leqslant$
2	66	–	–	–	–	–	1909	67
3	42	–	–	–	–	–	2304	42
5	30	2	0	0	1	1	3417	30
7	24	3	−1	0	1	−1	2391	24
11	18	5	0	−2	2	−1	1443	18
13	18	6	0	1	1	−2	3196	18

因此 $m(x\cdot y\cdot z)\leqslant 67$. 其次对 $X_0=67$ 及 μ 重复步骤, 如下表. 我们发现

p	μ	γ_0^*	γ_1^*	γ_2^*	γ_3^*	γ_4^*	$\iota(\Gamma_\mu^*)>$	$ord_p(x\cdot y\cdot z)\leqslant$
2	55	–	–	–	–	–	364	56
3	35	–	–	–	–	–	301	35
5	25	2	1	1	1	0	622	25
7	20	3	−1	1	−1	0	693	20
11	15	5	−1	−2	2	2	192	15
13	15	6	−1	0	3	−2	658	15

因此 $m(x\cdot y\cdot z)\leqslant 56$.

为了求出(6.2)在上表给出 $ord_p(x\cdot y\cdot z)$ 的界之下的解, 我们导出下面程序. 假定我们此刻感兴趣于找出满足 $ord_p(x\cdot y\cdot z)\leqslant f(p)$ 的解, 其中 $f(p)$ 对 $p=2,3,\cdots,13$ 是给定的. 选取 p

及 $\mu<f(p)-\mu_0$，并考虑对这些 p,μ 值的格 Γ_μ^*. 若(6.2)的满足于 $\mathrm{ord}_p(z)\geqslant\mu+\mu_0$ 的解 x,y,z 存在，则对 $i=0,\cdots,4$，满足 $x_i=\mathrm{ord}_{p_i}(x/y)$ 的向量 $[x_1,\cdots,x_4,x_0]^T$ 在格中. 其长度被 $\sqrt{f^2(p_0)+\cdots+f^2(p_4)}$ 界定. Γ_μ^* 中长度在这个界之下的所有向量可用 3.6 节中给出的 Fincke 和 Pohst 运算来求出. 则(6.2)对应于格点的所有解可挑选出来. 然后用 $\mu+\mu_0-1$ 取代 $f(p)$，并对重新选择的 p,μ 重复这过程.

我们完成这个程序，始于上表对 $f(p)$ 给出的关于 $\mathrm{ord}_p(x\cdot y\cdot z)$ 的界，以及第 6.7 节表Ⅳ的 p,m(其中$_非$位于(5.2)的解数由其阶求出). 结束于得到 $f(2)=4$，$f(p)=1$，$p=3,\cdots,13$. 剩下的解用手算可求出.

注　1. 定理 6.2 和 6.3 已应用于群论(参考 Alex[2]). 我们在 7、2 节中用定理 6.3.

2. 计算机计算对定理 6.3 的证明取 436 秒. 其中 412 秒用于第一简化步骤. 在这第一步骤中，我们在 11 步中应用 L^3 - 运算(见 3.5 节)，每格花费了约平均 60 秒. 剩下的 50 秒主要用于 24 个 $\theta^{(\mu)}$ 的计算.

6.6　关于 abc - 猜想的例

设 x,y,z 是正整数. 令

$$G=\prod_{\substack{p\mid xyz\\ p\text{是素数}}} p$$

对所有满足 $(x,y)=1$ 且 $x+y=z$ 的 x,y,z，定义

$$c(x, y, z) = \log z / \log G$$

Tijdeman[119]将它称为 Masser－比率．1987 年，Oesterlé[88]提出了决定是否存在一个绝对常数 C 使得对所有 x, y, z 都有 $c(x, y, z) < C$ 的问题．Masser[77]猜想一个强的结论：当 z 超过某个对所有 $\varepsilon > 0$ 仅依赖于 ε 的界时，有 $c(x, y, z) < 1 + \varepsilon$．有关的结果和猜想的综述，可参见 Stewart 和 Tijdeman[111]，Vojta[128]，Tijdeman[119]．目前关于 abc－猜想的最好结果是由 Stewert 和于坤瑞[112]得到的，他们证明了：存在可有效计算的绝对常数 C_1、C_2，可使

$$\log z < C_1 G^{2/3 + C_2/\log\log G}.$$

对以经验为依据的关于 $c(x, y, z)$ 方面的某些结果以及搜寻一般的 x, y, z 是令人感兴趣的．由前节已明显看出，这样的 x, y, z 对应于适当的 p－adic 逼近格中相对地短向量．

作为证明定理 5.5 和 6.3 的附带结果，我们计算 $c(x, y, z)$ 的值，在完成 Fincke 和 Pohst 的运算中我们发现相应的许多短向量．我们发现满足 $c(x, y, z) \geq 1.4$ 的例子列在下面．我们的寻找是相当无系统的，因此，我们不能保证列出的在任何意义下是完整的．

x	y	z	c(x, y, z)
11^2	$3^2 5^6 \cdot 7^3$	$2^{21} \cdot 23$	1.62599
1	$2 \cdot 3^7$	$5^4 \cdot 7$	1.56789
7^3	3^{10}	$2^{11} \cdot 29$	1.54708
$5^2 \cdot 7937$	7^{13}	$2^{18} \cdot 3^7 \cdot 13^2$	1.49762
11^2	$3^9 \cdot 13$	$2^{11} \cdot 5^3$	1.48887

x	y	z	c(x, y, z)
37	2^{15}	$3^8 \cdot 5$	1.48291
$2^7 \cdot 5^2$	$7^6 \cdot 41$	13^6	1.46192
1	$2^5 \cdot 3 \cdot 5^2$	7^4	1.45567
$2^{19} \cdot 13 \cdot 103$	7^{11}	$3^{11} \cdot 5^3 \cdot 11^2$	1.45261
1	$2^{12} \cdot 5^3$	$3^5 \cdot 7^2 \cdot 43$	1.44331
1	$2^4 \cdot 3^7 \cdot 547$	$5^8 \cdot 7^2$	1.43906
$2^{10} \cdot 7$	5^7	$3^8 \cdot 13$	1.43501
3	5^3	2^7	1.42657
5	3^{11}	$2^{10} \cdot 173$	1.41268

满足 $c(x, y, z) \geqslant 1.4$ 的两个另外的例子已知为:

$$x = 1, y = 3 \cdot 5 \cdot 47^2, z = 2^{18} \cdot 79, c(x, y, z) = 1.44965,$$

这由 G. Frey 发现的, 另外

$$x = 2, y = 109 \cdot 3^{10}, z = 23^5, c(x, y, z) = 1.62991$$

是由 E. Reyssat 发现的. 注意这两个例子在两个位置显示大素数.

这些结果对 abc－猜想的正确或不正确似乎得不到任何启发的迹象.

6.7 表

Table 1: (Theorem 6.2.)

$p = 2, p_0 = 3, p_1 = 5$

x_0	$p_0^{x_0}$	x_1	$p_1^{x_1}$	sign	u	w
2	9	10	9765625	−1	4	−610351
10	59049	10	9765625	−1	4	−606661
4	81	12	244140625	−1	9	−476837
6	729	10	9765625	−1	5	−305153
2	9	8	390625	−1	3	−48827
6	729	8	390625	−1	3	−48737
10	59049	8	390625	−1	3	−41447
14	4782969	10	9765625	−1	7	−38927
4	81	8	390625	−1	4	24409
0	1	8	390625	−1	5	−12207
8	6561	8	390625	−1	6	−6001
0	1	6	15625	−1	3	−1953
4	81	6	15625	−1	3	−1943
8	6561	6	15625	−1	3	−1133
6	729	6	15625	−1	4	−931
2	9	4	625	−1	3	−77
2	9	6	15625	−1	8	−61
0	1	4	625	−1	4	−39
4	81	4	625	−1	5	−17
0	1	2	25	−1	3	−3
2	9	2	25	−1	4	−1
1	3	1	5	1	3	1
1	3	3	125	1	7	1
2	9	0	1	−1	3	1
3	27	1	5	1	5	1
4	81	0	1	−1	4	5
4	81	2	25	−1	3	7
6	729	2	25	−1	6	11
6	729	4	625	−1	3	13
3	27	3	125	1	3	19
5	243	3	125	1	4	23
5	243	1	5	1	3	31
7	2187	5	3125	1	6	83
6	729	0	1	−1	3	91

x_0	$p_0^{x_0}$	x_1	$p_1^{x_1}$	sign	u	w
7	2187	1	5	1	4	137
11	177147	1	5	1	10	173
3	27	5	3125	1	4	197
8	6561	0	1	−1	5	205
7	2187	3	125	1	3	289
8	6561	4	625	−1	4	371
1	3	5	3125	1	3	391
5	243	5	3125	1	3	421
9	19683	3	125	1	5	619
8	6561	2	25	−1	3	817
10	59049	6	15625	−1	5	1357
5	243	7	78125	1	5	2449
9	19683	1	5	1	3	2461
9	19683	5	3125	1	3	2851
10	59049	2	25	−1	4	3689
12	531441	4	625	−1	7	4147
1	3	7	78125	1	4	4883
9	19683	7	78125	1	4	6113
13	1594323	7	78125	1	8	6533
10	59049	4	625	−1	3	7303
10	59049	0	1	−1	3	7381
12	531441	8	390625	−1	4	8801
3	27	7	78125	1	3	9769
7	2187	7	78125	1	3	10039
11	177147	5	3125	1	4	11267
3	27	9	1953125	1	7	15259
11	177147	3	125	1	3	22159
11	177147	7	78125	1	3	31909
12	531441	0	1	−1	4	33215
12	531441	6	15625	−1	3	64477
12	531441	2	25	−1	3	66427
11	177147	9	1953125	1	5	66571
13	1594323	3	125	1	4	99653
7	2187	9	1953125	1	4	122207
14	4782969	2	25	1	5	149467
13	1594323	1	5	1	3	199291
13	1594323	5	3125	1	3	199681

x_0	$p_0^{x_0}$	x_1	$p_1^{x_1}$	sign	u	w
1	3	9	1953125	1	3	244141
5	243	9	1953125	1	3	244171
9	19683	9	1953125	1	3	246601
14	4782969	6	15625	−1	4	297959
13	1594323	9	1953125	1	3	443431
15	14348907	5	3125	1	5	448501

$p = 3, p_0 = 2, p_1 = 5$

x_0	$p_0^{x_0}$	x_1	$p_1^{x_1}$	sign	u	w
14	4782969	8	390625	−1	3	549043
14	4782969	4	625	−1	3	597793
14	4782969	0	1	−1	3	597871
16	43046721	0	1	−1	6	672605
9	19683	11	48828125	1	6	763247
15	14348907	1	5	1	4	896807
14	16384	10	9765625	−1	4	−120361
9	512	9	1953125	−1	3	−72319
4	16	8	390625	−1	3	−14467
12	4096	6	15625	−1	3	−127
7	128	5	3125	−1	4	−37
2	4	4	625	−1	3	−23
1	2	2	25	1	3	1
5	32	1	5	−1	3	1
6	64	3	125	1	3	7
11	2048	4	625	1	5	11
9	512	0	1	1	3	19
10	1024	2	25	−1	3	37
3	8	6	15625	1	4	193
15	32768	3	125	−1	4	403
14	16384	1	5	1	3	607
17	131072	7	78125	−1	3	1961
16	65536	5	3125	1	3	2543
8	256	7	78125	1	3	2903
19	524288	2	25	1	4	6473
18	262144	0	1	−1	3	9709
23	8388608	1	5	−1	6	11507
13	8192	8	390625	1	3	14771

x_0	$p_0^{x_0}$	x_1	$p_1^{x_1}$	sign	u	w
22	4194304	8	390625	−1	5	15653
10	1024	11	48828125	1	7	22327
18	262144	9	1953125	1	4	27349
20	1048576	4	625	−1	3	38813
0	1	9	1953125	1	3	72338
21	2097152	6	15625	1	3	78251
5	32	10	9765625	1	3	361691
24	16777216	3	125	1	3	621383
23	8388608	10	9765625	1	3	672379
26	67108864	7	78125	1	4	829469

$p=5,\ p_0=2,\ p_1=3$

x_0	$p_0^{x_0}$	x_1	$p_1^{x_1}$	sign	u	w
12	4096	16	43046721	−1	3	−344341
5	32	15	14348907	−1	3	−114791
7	128	1	3	−1	3	1
6	64	8	6561	1	3	53
14	16384	2	9	−1	3	131
13	8192	9	19683	1	3	223
20	1048576	10	59049	1	3	8861
21	2097152	3	27	−1	3	16777

Table IV.

nr.	p	m	#
1	2	44	–
2	3	28	–
3	5	20	–
4	7	16	–
5	11	12	–
6	13	12	–
7	2	33	–
8	3	21	–
9	5	15	–
10	7	12	–
11	11	9	–
12	3	9	–
13	2	22	–
14	3	14	–
15	5	10	–
16	7	8	–
17	11	6	–
18	13	6	–
19	2	21	–
20	2	20	–
21	2	19	–
22	2	18	–
23	2	17	–
24	2	16	–
25	2	15	–
26	2	14	–
27	2	13	1
28	2	12	2
29	2	11	2
30	3	13	–
31	3	12	–
32	3	11	
33	3	10	1
34	3	9	1
35	3	8	1
36	3	7	6
37	5	9	
38	5	8	
39	5	7	–
40	5	6	
41	5	5	6
42	7	7	–
43	7	6	
44	7	5	1
45	7	4	4
46	11	5	–
47	11	4	1
48	11	3	4
49	13	5	–
50	13	4	–
51	13	3	1
52	2	10	2
53	2	9	3
54	2	8	6
55	2	7	15
56	2	6	16
57	2	5	26
58	2	4	31
59	2	3	44
60	3	6	5
61	3	5	8
62	3	4	16
63	3	3	35
64	3	2	54
65	3	1	87
66	5	4	1
67	5	3	5
68	5	[illegible]	18
69	5	1	30
70	7	3	
71	7	2	6
72	7	1	18
73	11	2	1
74	11	1	5
75	13	2	–
76*	13	1	4

Table II. (Theorem 6.3)

x	y	z	$\text{ord}_p(x)$ p=2	3	5	7	11	13	$\text{ord}_p(y)$ p=2	3	5	7	11	13	$\text{ord}_p(z)$ p=2	3	5	7	11	13
2401	4160	6561	0	0	0	4	0	0	6	0	1	0	0	1	0	8	0	0	0	0
875	6561	7436	0	0	3	1	0	0	0	8	0	0	0	0	2	0	0	0	1	2
1183	6561	7744	0	0	0	1	0	2	0	8	0	0	0	0	6	0	0	0	2	0
1125	8192	9317	0	2	3	0	0	0	13	0	0	0	0	0	0	0	0	1	3	0
1183	8192	9375	0	0	0	1	0	2	13	0	0	0	0	0	0	1	5	0	0	0
16	14625	14641	4	0	0	0	0	0	0	2	3	0	0	1	0	0	0	0	4	0
81	14560	14641	0	4	0	0	0	0	5	0	1	1	0	1	0	0	0	0	4	0
1936	13689	15625	4	0	0	0	2	0	0	4	0	0	0	2	0	0	6	0	0	0
3718	11907	15625	1	0	0	0	1	2	0	5	0	2	0	0	0	0	6	0	0	0
5824	9801	15625	6	0	0	1	0	1	0	4	0	0	2	0	0	0	6	0	0	0
49	16335	16384	0	0	0	2	0	0	0	3	1	0	2	0	14	0	0	0	0	0
2695	13689	16384	0	0	1	2	1	0	0	4	0	0	0	2	14	0	0	0	0	0
8019	8788	16807	0	6	0	0	1	0	2	0	0	0	0	3	0	0	0	5	0	0
3584	14641	18225	9	0	0	1	0	0	0	0	0	0	4	0	0	6	2	0	0	0
1625	16807	18432	0	0	3	0	0	1	0	0	0	5	0	0	11	2	0	0	0	0
3993	16807	20800	0	1	0	0	3	0	0	0	0	5	0	0	6	0	2	0	0	1
49	28512	28561	0	0	0	2	0	0	5	4	0	0	1	0	0	0	0	0	0	4
12936	15625	28561	3	1	0	2	1	0	0	0	6	0	0	0	0	0	0	0	0	4
22000	6561	28561	4	0	3	0	1	0	0	8	0	0	0	0	0	0	0	0	0	4
15625	17303	32928	0	0	6	0	0	0	0	0	0	0	3	1	5	1	0	3	0	0
507	32768	33275	0	1	0	0	0	2	15	0	0	0	0	0	0	0	2	0	3	0
10985	41503	52488	0	0	1	0	0	3	0	0	0	3	2	0	3	8	0	0	0	0
10000	49049	59049	4	0	4	0	0	0	0	0	0	3	1	1	0	10	0	0	0	0
14641	46875	61516	0	0	0	0	4	0	0	1	6	0	0	0	2	0	0	1	0	3
7168	78125	85293	10	0	0	1	0	0	0	0	7	0	0	0	0	8	0	0	0	1
20449	97200	117649	0	0	0	0	2	2	4	5	2	0	0	0	0	0	0	6	0	0
13	151250	151263	0	0	0	0	0	1	1	0	4	0	2	0	0	2	0	5	0	0
12005	161051	173056	0	0	1	4	0	0	0	0	0	0	5	0	10	0	0	0	0	2
121	255879	256000	0	0	0	0	2	0	0	9	0	0	0	1	11	0	3	0	0	0
2197	853443	585640	0	0	0	0	0	3	0	5	0	4	0	0	3	0	1	0	4	0
91	1771470	1771561	0	0	0	1	0	1	1	11	1	0	0	0	0	0	0	0	6	0

Table III.

$-\log_2 5/\log_2 3$

0.10101 11101 00001 11110 11000 10101 00000 01001 11101 00010 10000 10011 10110 10000 01011 11100 00001 11010 00000 00001
00010 11100 11100 10111 01001 01101 11000 01010 01110 01010 11110 00000 00101 00110 00100 00011 01111 01110 01010 11101
10010 01001 00001 10100 00111 00001 11111 01111 00011 10110 00000 00101 01101 01100 00010 01110 11100 11101 11011 01011
10111 00100 11111 00100 00100 10001 10010 01011 10010 01101 00000 01100 01111 10111 01101 00110 11110 00000 01100 11010
00001 00111 11011 11001 01000 10000 00110 11011 11001 01000 01110 11001 00010 00010 11000 01000 00110 01100 11101 11110
00000 11101 10101 11100 10010 11101 01011 10001 01100 11000 01100 00110 01001 01100 01000 01001 10001 11000 01101 10100
00110 00011 0111...

$-\log_2 7/\log_2 3 =$

0.01001 01011 01111 11100 11010 01111 11111 10010 01000 11100 00011 00100 01011 11110 00101 11010 11110 10001 00000 01110
01011 00101 10010 00111 10111 01001 10001 11000 11011 10111 01011 01001 01011 00100 11001 11000 10111 01100 00001 01110
11000 01011 00011 01110 10000 01101 11000 11001 00010 00011 01100 11110 11010 11110 00001 10110 01010 00001 01000 11011
10010 01000 00011 01011 10010 11001 10000 01101 10111 01001 01000 00101 00011 11001 10000 00011 00101 00100 00000 10011
11100 01110 11110 10101 00101 01110 11100 10000 01011 00100 01100 11100 00100 01110 10001 00001 10000 00111 10111 00011
10111 01100 10110 00111 00101 10011 01100 11111 00101 01011 11101 11011 01011 10110 01100 10001 11011 01100 01001 11111
10001 11110 1010...

$-\log_2 11/\log_2 3 =$

0.10011 01110 00001 01001 00110 01010 01110 00100 00101 10000 01000 11001 10010 01111 10110 00011 00101 01110 00111 11101
10100 01101 01101 10111 10110 01100 10110 11110 00000 11000 01000 11111 10010 10011 10110 01001 01111 00101 00011 11100
01100 10100 01000 10101 00010 01011 10111 10000 00001 01000 11010 01010 11010 11100 00001 10110 01001 11111 11110 10010
11101 11100 10010 00100 11000 00000 01110 10100 00101 10010 10010 10010 01111 10100 01001 10111 01000 10101 01110 01000
11001 11001 10011 11110 10000 11001 10110 10101 00010 11100 11101 11011 10110 00111 01010 11000 01000 10111 11110 10010
10101 11100 11011 001111 11000 00111 11100 01101 11100 01101 00001 00100 01001 11000 01101 10101 00110 10101 00001 00001
10101 11001 1111...

$\log_2 13/\log_2 3 =$

0 11011 10110 10100 10001 01100 01111 10001 00110 01110 00001 01110 01011 11101 10110 11100 00111 11111 11001 11011 11110
00011 11110 01000 10010 11011 11101 01000 11000 11111 01011 00001 10101 00110 00000 00001 01101 10010 00101 00100 10101
01011 11100 10011 11011 00000 01110 10100 00011 10000 11101 00010 00000 10011 01011 11011 10000 11010 10010 11010 00100
10010 00001 01000 10101 10110 01001 01000 11111 01101 00111 11100 10001 01110 11000 01010 10011 11001 01111 01111 00001
10011 00000 00101 10111 11100 01011 01011 01011 11000 10001 11110 01000 10110 00011 11011 11011 11010 11110 10100 01110
01000 00111 00000 00000 00011 10111 11111 10100 01111 10010 01100 10101 00111 10110 11010 01111 10000 11101 10111 10001
00000 01100 1001. . .

$\log_3 5/\log_3 2 =$

0 11022 12121 22001 12010 21102 10210 10022 20212 20010 10112 22201 21021 21022 10000 22020 12012 02022 21001 00012 02020
21210 12202 12200 00000 10120 00211 12021 10120 02100 10222 22122 01201 21111 11121 11001 20222 10000 20121 22221 01002
20220 12211 22211 00100 20202 00012 11112 10122 21001 21200 12201 12220 11100 01102 20010 11102 10222 00020 21202 21112
20201 21100 11212 22222 21120 02020 12121 02122 11111 10001 10220 21022 10012 11212 20001 10211 02120 02122 1. . .

$-\log_3 7/\log_3 2 =$

0.20101 10202 20011 12121 01102 11100 01210 20120 02122 02012 20202 00121 21200 01201 11120 11211 11212 22100 00100 22201
20021 11112 01122 00011 22100 00000 22011 11100 12010 22110 12122 00222 10220 21102 20001 02101 00121 11002 11012 12201
21011 20100 01110 02000 21222 12010 02201 22012 01022 02021 00210 10221 00221 20202 02222 22122 00100 12021 21220 02220
20000 00002 00111 11221 11002 20102 12212 12012 22122 00211 01210 01102 21010 20121 01020 11111 20002 10122 2 . . .

$-\log_3 11/\log_3 2 =$

0.21112 20101 00222 20222 01212 01100 12100 01201 01111 01212 01210 20121 20001 12021 01122 21202 12020 00212 11102 11002
01001 10200 22202 02001 20022 10221 00010 10011 22220 01021 02121 00211 22210 21101 22012 11111 02010 00221 00102 20111
20202 01201 01220 22022 11221 10121 10202 10011 11002 10220 22110 21121 00112 02122 21200 01021 21002 21002 10010 00110
00101 12202 12000 21012 11010 11020 00222 00012 11201 11010 00122 01120 22200 20112 12122 10202 01211 00210 2. . .

$-\log_3 13/\log_3 2 =$

0.10221 02211 12122 22010 10002 01221 00121 02020 11201 02021 02112 21010 20122 02001 02112 21012 10222 01002 01200 01211

10111 21100 12121 11010 02000 02212 11111 21220 22020 02000 01222 12112 02100 10110 20002 10222 02112 20112 11100 00211
20012 11102 22220 00112 00001 11110 11102 22201 01122 22211 22201 11011 22201 01200 22121 02101 22222 22002 01010 01021
12020 20111 12102 00011 02002 02000 10211 00222 12202 02202 20212 22012 01222 20220 11211 20021 11111 00000 2.

$-\log_5 3/\log_5 2$

0.33002 02003 04411 23120 44012 01011 00044 43204 30340 00023 14333 12413 43420 40302 10202 44104 32433 24432 03021 12311
34044 40231 04112 33230 00242 14232 14400 31104 42112 44033 11014 44344 12114 44211 32120 43131 34041 00411 34233 41410
24120 42032 43014 21421 40044 01142 21004 42021 14011 10404 00214 31110 04441 42431 24423 0243

$-\log_5 7/\log_5 2 =$

0.03044 34433 10114 43203 12033 14002 12341 31312 03421 00343 41423 00040 24241 22103 14240 32214 11401 42230 13040 33404
04310 43034 13233 23241 43002 44411 41124 22443 42412 30420 11223 43101 01000 42112 10443 34210 03410 14414 02220 24443
13332 33123 23331 20323 44440 13210 14403 32122 03040 31123 04212 22443 44223 23133 02003 1240.

$-\log_5 11/\log_5 2$

0.44032 21012 13124 21134 03320 33422 21041 12112 42420 00220 41143 12040 32144 21100 01304 24013 43401 23313 12022 34404
12413 10214 30123 11014 24110 42444 42030 02413 20241 22304 23423 13414 03234 30000 10334 44322 00330 01104 44410 44113
31022 33142 14441 44113 21413 23132 31413 32032 01221 40210 24101 30133 13110 13400 22110 2334.

$-\log_5 11/\log_5 2$

0 12423 02224 01323 24314 23021 32420 14134 41224 04403 11334 43213 333303 03130 32244 11133 43243 23422 11320 41041 31134
41320 34310 03024 40012 23213 10014 41441 04420 40114 00021 33224 30103 03243 32031 22021 20234 32441 00013 04203 43134
22012 30332 22422 43110 13302 34431 13241 13230 44204 14432 33210 24121 13144 03230 14301 3040 .

$-\log_7 2/\log_7 3 =$

0 20603 14521 11264 52354 45364 60036 13515 13044 46363 40432 02366 04135 21304 53356 32205 44546 66301 00123 63633 04024
40631 53516 64053 50031 26436 46625 03465 02235 11551 46123 25164 52364 25520 12240 64220 00164 43634 02066 41264 61233
41326 32413 65633 52502 526.

$\log_7 5/\log_7 3$ =

0.62250 55002 24045 66544 01041 43506 34535 04453 26545 45453 33[illegible] [illegible] 353 55530 22443 10105 55002 62520 33063 16320 22253
42306 51054 13301 06465 43020 41555 41121 64255 11350 55053 64515 44465 36222 25605 66346 16142 31340 45522 31033 14255
21343 24510 62633 00155 361. . . .

$-\log_7 11/\log_7 3$ =

0.25035 56505 33553 02331 10224 32143 50543 02561 42352 23450 26326 53446 23462 51210 02416 02335 13066 54240 13006 60451
00441 56630 66142 56540 44042 52255 15314 10131 40626 10543 [illegible] 04254 45066 50232 65102 41555 41254 02211 54156 34054
41366 64215 64014 56645 550. .

$-\log_7 13/\log_7 3$ =

0.21305 11055 56501 22565 55610 32506 13150 66465 56420 [illegible] [illegible] 16426 11613 41010 66512 26566 50652 02025 40431 56566
43655 56120 34610 53642 61544 36122 61225 42410 23035 [illegible] 26220 14444 23632 33426 15605 51104 34116 04520 65502 65542
24255 36603 45452 66563 536. . .

$-\log_{11} 3/\log_{11} 2$ =

0.08248 A4245 06166 43468 58202 44A56 73171 16758 A203A 8A543 28431 86731 11411 4A296 993A7 31A79 00421 95444 80670 57433
59439 78064 34745 1A710 64682 08044 81761 27049 03452 3661A 40979 29601 898A4 50. .

$-\log_{11} 5/\log_{11} 2$ =

0.551A9 7223A 31378 09193 42445 306A3 96588 11862 48667 AA6A2 39A03 77139 01693 21678 33652 12687 95AA8 24190 78276 28711
08399 68022 2A607 55A17 2231A 80798 76947 73936 21835 30A1A 95324 1A8A3 82999 67

$-\log_{11} 7/\log_{11} 2$ =

0.44804 92167 71327 83472 37453 00781 3256A 2A367 85671 88907 799A1 4AAAA 784A1 29329 A6950 17481 86846 17379 94130 77091
29354 33161 9A146 03746 52A14 20214 22541 58A91 50337 7954A 89A01 43809 A8152 52

$-\log_{11} 13/\log_{11} 2$ =

0.9011A 94962 52990 39096 3A68A 7556A 1A4A3 44758 57692 20188 42770 072A3 9A977 8819A 97518 14396 07360 899A2 99391 26176
84077 81181 54473 58532 58A01 91643 28056 63940 99265 27989 37450 85913 91289 56

$-\log_{13}3/\log_{13}2 =$

0.621B5 15581 0A077 3B5C8 49202 39A32 82105 848C7 70988 B863B 75151 52114 5C25A 04902 6B6C7 377B9 3122B 5CAC0 13945 A2471 9B4BA A79C2 7A91C 5A989 C392A CC16A A20A1 75C6B 06BB6 8A3B9 C782B AA70C AB218 C9

$-\log_{13}5/\log_{13}2 =$

0.44570 79C51 73665 3796C B7C61 335A0 79906 2B429 51211 4900B 481B1 621AB 2AC77 C2291 1662A BB03A 8CB9C 77331 74992 11C07 BB101 10301 77310 B8B28 83AB2 57975 7C697 57928 23B72 297CB 0A414 32B3C A67A8 48…

$-\log_{13}7/\log_{13}2 =$

0.A1C78 9C71A 63110 51424 42CA9 0AAA7 B225B B0281 501B1 976C2 3C05B 09CA3 AB803 C3251 838AC 72502 A1844 03603 644A8 A8501 173BB BBC1C 30466 223C6 C98B4 564C2 47140 28856 C8676 15C30 12892 A3317 163C8 CA

$-\log_{13}11/\log_{13}2 =$

0.1760A A080C 20874 BB876 B2162 75989 CB19B B7CC2 26BB7 87093 5A833 A9375 AB4BA 8C0BC 1A698 96C6B A9411 34B75 4B718 63BC3 571A9 14566 8819B A4B95 B4244 452A8 29623 49AA5 CB804 AC61A CC513 08855 79185 43

第七章　两个 S－单位的和是平方数问题

7.1　导言

设 $p_1,\cdots,p_s(s\geqslant 1)$ 是不同素数，S 是没有不同于 p_i 的素因子的正有理数集合．一个有理数称为一个 S－单位，若其绝对值是 S 中元素的一个商．因此 S－单位集合是

$$\{\pm p_1^{x_1}\cdot\cdots\cdot p_s^{x_s}\mid x_i\in Z, i=1,\cdots,s\}.$$

我们研究丢番图方程

$$x+y=z^2,$$

x，y 是 S－单位，$z\in Q$，这里素数 $p_1,\cdots,p_s$ 的集合是给定的．我们表明如何运用 p－adic 对数线性型理论以及计算的 p－adic 丢番图逼近方法来求出这方程的全部解．对 $\{p_1,\cdots,p_s\}=\{2,3,5,7\}$ 完整地解方程，我们实际完成所有必要的计算．这种类型的方程已应用于计算的代数几何（看 Setzer[105]，Pinch[95]）．

我们从去掉分母开始．设 x，y，z 是一组解．存在一个 $d\in S$，使得 $|d\cdot x|,|d\cdot y|\in S$．令 $d=d_1\cdot d_2^2$，其中 $d_1,d_2\in S$ 且 d_1 非平方数．则

$$d_1\cdot d\cdot x+d_1\cdot d\cdot y=(d_1\cdot d_2\cdot z)^2,$$

这与 $x+y=z^2$ 形式相同，只不过现在 $|d_1\cdot d\cdot x|,|d_1\cdot d\cdot y|\in S$

$\subset Z$ 且 $d_1 \cdot d_2 \cdot z \in Z$. 不失一般性, 我们因此可研究

$$x + y = z \tag{7·1}$$

其中

$$\begin{cases} x \in S, \pm y \in S, z \in Z, \\ x \geqslant y, z > 0 \\ (x, y) \text{非平方数} \end{cases} \tag{7·2}$$

我们将证明下面结果.

定理 7·1　设 $p_1, \cdots, p_s$ 给定. 存在一个有效可计算常数 C. 仅依赖于 $p_1, \cdots, p_s$, 使得方程(7·1)连同条件(7·2)的任意解满足 $\max(x, |y|, z) < C$.

这理 7·2　设 $\{p_1, \cdots p_s\} = \{2, 3, 5, 7\}$. 满足条件(7·2)的方程(7·1)恰有 388 个解在第 7·9 节表 I 给出.

注: 1. 我们强调本章的目的不仅是证明这些定理, 而且也表明对任意给定的素数集 $\{p_1, \cdots, p_s\}$, 类似于定理 7·2 的结果可沿着相同的路线证明, 其计算方法或更多或更少.

2. 方程(7·1)连同条件(7·2)可看作是一般 Ramanujan - Nagell 方程

$$x^2 + k = p_1^{n_1} \cdot \cdots \cdot p_s^{n_s} \tag{7·3}$$

的进一步推广(看第四章), 即用任取的 $|k| \in S$ 代表固定的 $k \in Z$. 本章解(7·1)的方法也是第四章中解(7·3)的方法的一种推广.

方程(7·1)可变换成若干 Pell - 型方程. 设

$$x = D \cdot u^2,$$

其中 D, $u \in S$, D 非平方数. D 只有 2^s 多种可能. 现在, (7·1) 等价于有限多个方程

$$z^2 - D \cdot u^2 = y \tag{7·4}$$

其中 $u \in S$, $\pm y \in S$, $z \in Z$ 满足 $z > 0$ 且 $(u, y) = 1$. 我们处理方程(7·4)采用将其两边在域 $K = Q(\sqrt{D})$ 中分解因子的方法. 当论及方程(7·4)时我们容许 z 和 u 是负数.

7.2 D=1 的情形

首先我们考虑 D=1 的特殊情形. 则(7·4)等价于

$$\begin{cases} z + u = y_1 \\ z - u = y_2 \end{cases},$$

其中 $y = y_1 \cdot y_2$, $y_1 \in S$, $\pm y_2 \in S$, $y_1 > |y_2|$. 作减法计算导出

$$2u = y_1 - y_2 \tag{7·5}$$

现在, 所有变量 u, y_1, y_2(除去符号)都属于 S, 因而在 Z 中. 由 $(u, y_1) = (u, y_2) = 1$, 方程(7·5)形如 $a + b = c$ 或 $2 \cdot a + 2 \cdot b = 2 \cdot c$, 其中 a、b、c 仅由素数 2, p_1, …, p_s 组成, 且 $(a, b) = 1$, $a \geq b > 0$. 第六章已示范解方程 $a + b = c$: 作为一般例子 $\{p_1, \cdots, p_s\} = \{2, 3, 5, 7\}$, 我们有下面结果.

引理 7·3 设 $\{p_1, \cdots, p_s\} = \{2, 3, 5, 7\}$. 满足条件(7·2)及

$D=1$ 的方程(7·1)恰有 95 个解在第 7·9 节表 I 中满足 $D=1$ 部分给出.

证明　由定理 6·3 导出, $a+b=c$, 满足 $a、b、c\in S$, $(a,b)=1$, $a\geqslant b$, 恰好有 63 个解. 这些解容易计算. 每个解对(7·5)发生三种可能:

若 $2|a$, 则 $(u, y_1, y_2)=(\frac{1}{2}a, b, c), (b, 2c, 2a), (c, 2a, -2b)$;

若 $2|b$, 则 $(u, y_1, y_2)=(a, 2b, 2c), (\frac{1}{2}b, c, a), (c, 2a, 2b)$;

若 $2|c$, 则 $(u, y_1, y_2)=(a, 2b, 2c), (b, 2c, 2a), (\frac{1}{2}c, a, -b)$;

由此得到 189 种可能, 95 个满足 $x\geqslant y$ 和 $z>0$ 在表 I 中 $D=1$ 部分给出, 除此之外, 其余不满足.

这就完成 $D=1$ 的情形的论述.

7.3　对于一般递归

从现在起, 设 $D>1$. 令 $K=Q(\sqrt{D})$, 设 $\sigma: K\rightarrow K$ 是 K 的自同构, 满足 $\sigma(\sqrt{D})=-\sqrt{D}$. 对 K 中任意数或理想 X, 为方便起见, 我们将 $\sigma(X)$ 写成 X'. 对 $i=1, \cdots, s$, 设 $\mathfrak{p}_i$ 是 K 中的素理想使得 $\mathrm{ord}_{p_i}(\mathfrak{p}_i)>0$. 若 p_i 在 O_k 中分裂, 这正好定义为若对 $\sqrt{D}\pmod p$ 的两种可能已得到选择. 对(7·4)的解 z, u, y 设

$$x=z+u\cdot\sqrt{D}$$

则 $y=x\cdot x'$，由 $(u,y)=1$，有

$$\min[\mathrm{ord}_{p_i}(u),\mathrm{ord}_{p_i}(y)]=0 \tag{7·6}$$

方程(7·4)导出共轭理想方程

$$\begin{cases}(x)=\prod_{i=1}^{s}\mathfrak{p}_i^{a_i}\cdot\mathfrak{p}_i'^{b_i}\\(x')=\prod_{i=1}^{s}\mathfrak{p}_i'^{a_i}\cdot\mathfrak{p}_i^{b_i}\end{cases} \tag{7·7}$$

其中 $a_i,b_i\in N_0$，且当 $\mathfrak{p}_i=\mathfrak{p}_i'$ 时，$b_i=0$. 我们需要下面辅助引理.

引理 7·4 若 $\xi\in K$ 且对素数 p，$\mathrm{ord}_p(\xi)=\mathrm{ord}_p(\xi')$，则

$$\mathrm{ord}_p(\xi)\leqslant\mathrm{ord}_p(\xi-\xi')$$

此外，若 $p=2$ 且 $D\equiv1(\mathrm{mod}\ 8)$，则

$$\mathrm{ord}_2(\xi)\leqslant\mathrm{ord}_2((\xi-\xi')/2),$$

若 $p=2$ 且 $D=2,3(\mathrm{mod}\ 4)$，则

$$\mathrm{ord}_2(\xi)\leqslant\mathrm{ord}_2((\xi-\xi')/2\sqrt{D})+\frac{1}{2}.$$

证明 这是不难的练习，留给读者.

我们对素数 p_i 在 K 中分解因子照例区别三种情况：分裂，分歧或仍是素数. 看 Borevich 和 Shafarevich[21]，节 Ⅲ. 8..

• p_i 仍是 K 中素数. 则 $p_i\nmid D$，且当 $p_i=2$ 时，有 $D\equiv5(\mathrm{mod}\ 8)$. 我们有 $(p_i)=\mathfrak{p}_i=\mathfrak{p}_i'$，又由 $\mathrm{ord}_{p_i}(x)=\mathrm{ord}_{p_i}(x')$ 及引理 7·4，得

$$\mathrm{ord}_{p_i}(y)=2\cdot\mathrm{ord}_{p_i}(x)\leqslant 2\cdot\mathrm{ord}_{p_i}(x-x')$$
$$=2\cdot\mathrm{ord}_{p_i}(2\cdot u\cdot\sqrt{D}.$$

运用(7·6)导出.

若 $p_i\neq 2$，则 $\mathrm{ord}_{p_i}(y)=2\cdot a_i=0$，

若 $p_i=2$，则 $\mathrm{ord}_2(y)=2\cdot a_i=0, 2$，又若 $a_i=1$，则 $\mathrm{ord}_2(u)=0$.

→p_i 在 K 中分歧. 若 $p_i\neq 2$，则 $p_i\mid D$，又若 $p_i=2$，则 $D\equiv 2, 3 \pmod 4$. 我们有 $(p_i)=\mathfrak{p}_i^2, \mathfrak{p}_i=\mathfrak{p}_i'$ 以及 $\mathrm{ord}_{p_i}(x)=\mathrm{ord}_{p_i}(x')=\frac{1}{2}\cdot a_i$. 由引理 7·4，我们发现

$$\mathrm{ord}_{p_i}(y)=2\cdot\mathrm{ord}_{p_i}(x)\leqslant 1+2\cdot\mathrm{ord}_{p_i}((x-x')/2\cdot\sqrt{D})$$
$$=1+2\cdot\mathrm{ord}_{p_i}(u).$$

由(7·6)得

$$\mathrm{ord}_{p_i}(y)=a_i=0.1, \text{且当 } a_i=1 \text{ 时}, \mathrm{ord}_{p_i}(u)=0.$$

→p_i 在 K 中分裂. 则 $p_i\nmid D$，且当 $p_i=2$ 时，$D\equiv 1 \pmod 8$. 我们有 $(p_i)=\mathfrak{p}_i\cdot\mathfrak{p}_i'.\mathfrak{p}_i\neq\mathfrak{p}_i'$. 进而，$\mathrm{ord}_{p_i}(\mathfrak{p}_i)=1, \mathrm{ord}_{p_i}(\mathfrak{p}_i')=0$. 因此 $\mathrm{ord}_{p_i}(x)=a_i, \mathrm{ord}_{p_i}(x')=b_i$. 若 $a_i=b_i$，则从

$$\mathrm{ord}_{p_i}(y)=2\cdot\mathrm{ord}_{p_i}(x)\leqslant 2\cdot\mathrm{ord}_{p_i}((x-x')/2)$$
$$=2\cdot\mathrm{ord}_{p_i}(u).$$

由(7·6)得

$$\mathrm{ord}_{p_i}(y)=a_i=b_i=0.$$

若 $a_i\neq b_i$，则 $\mathrm{ord}_{p_i}(y)=a_i+b_i>0$，因此 $\mathrm{ord}_{p_i}(u)=0$，由(7·6)，在此情形我们导出

$$\begin{aligned}\mathrm{ord}_{p_i}(y)=a_i+b_i&\geqslant 1+2\cdot\min(a_i,b_i)=1+2\cdot\mathrm{ord}_{p_i}(x-x')\\&=1+2\cdot\mathrm{ord}_{p_i}(2).\end{aligned}$$

随之有

若 $p_i\neq 2$，则 $\mathrm{ord}_{p_i}(y)=\max(a_i,b_i)$，$\min(a_i,b_i)=0$，

若 $p_i=2$，则 $\mathrm{ord}_{p_i}(y)=\max(a_i,b_i)+1$，$\min(a_i,b_i)=1$.

若 $p_i=2$，设 $b_0=\min(a_1,b_1)$，其余情形，设 $b_0=0$（注意 $\min(a_i,b_i)=1$ 仅当 $\mathfrak{p}_i\neq\mathfrak{p}_i'$ 时发生，因此仅当 $p_i=2$ 时分裂）. 让我们假定 $p_1,\cdots,p_s$ 的分裂素数是 $p_1,\cdots,p_t$，其中 $0\leqslant t\leqslant s$. 令

$$I=\{i\mid 1\leqslant i\leqslant t,\ a_i>b_i\},$$

$$I=\{i\mid 1\leqslant i\leqslant t,\ a_i<b_i\}.$$

对 $i=1,\cdots,t$，设 h_i 是使 $\mathfrak{p}_i^{h_i}$ 是一个素理想的最小正整数，比如说

$$\mathfrak{p}^{h_i}=(\pi_i).$$

若 h 表示 K 的类数，则 $h_i\mid h$. 现在，$\pi_i\in K$ 是该由用单位来乘的乘法运算所决定了的. 因此我们可选择 π_i 使得

$$|\pi_i| > |\pi_i'|, \text{若 } i \in I,$$

$$|\pi_i| < |\pi_i'|, \text{若 } i \in I'.$$

对 $i = 1, \cdots, t$, 令

$$|a_i - b_i| = c_i \cdot h_i + d_i,$$

满足 $c_i, d_i \in N_0$ 及 $0 \leqslant d_i \leqslant h_i - 1$. 考虑理想

$$\mathfrak{a} = (2)^{b_0} \cdot \prod_{i \in I} \mathfrak{p}_i^{d_i} \cdot \prod_{i \in I'} \mathfrak{p}_i'^{d_i} \cdot \prod_{i = t+1}^{s} \mathfrak{p}_i^{a_i}.$$

由上面考虑导出, 对于给定 $k, p_1, \cdots, p_s$, 关于 $\mathfrak{a}$ 仅存在有限多种可能. 由(7·7)导出

$$(x) = \mathfrak{a} \cdot \prod_{i \in I} (\pi_i)^{c_i} \cdot \prod_{i \in I'} (\pi_i')^{c_i}$$

(即, 若 $p_i \neq 2$, 则 $|a_i - b_i| = \max(a_i, b_i)$, 因此 $\min(a_i, b_i) = 0$; 若 $p_i = 2$ 且 $b_0 = 1$, 则 $|a_i - b_i| = \max(a_i, b_i) - 1$). 因此, $\mathfrak{a}$ 是一个主理想, 比如说, 对任意 $\alpha \in o_k$,

$$\mathfrak{a} = (\alpha)$$

直至用单位来乘, 对 α 仅存在有限多种可能. 设 ε 是 K 的基本单位, 满足 $\varepsilon > 1$. 现在, (7·7)导出方程组

$$\begin{cases} x = z + u\sqrt{D} = \pm\alpha\cdot\varepsilon^{n}\cdot\prod_{i\in I}\pi_i^{c_i}\cdot\prod_{i\in I'}\pi_i'^{c_i} \\ x' = z - u\sqrt{D} = \pm\alpha'\cdot\varepsilon'^{n}\cdot\prod_{i\in I}\pi_i'^{c_i}\cdot\prod_{i\in I'}\pi_i^{c_i} \end{cases}$$

其中 $n\in Z$. 设对于 $n\in Z, m_1, \cdots, m_t\in N_0$, 以及对于 α 的每种可能

$$G_\alpha(n, m_1, \cdots, m_t)$$

$$= \frac{\alpha}{2\sqrt{D}}\cdot\varepsilon^{n}\cdot\prod_{i\in I}\pi_i^{m_i}\cdot\prod_{i\in I'}\pi_i'^{m_i} - \frac{\alpha'}{2\sqrt{D}}\cdot\varepsilon'^{n}\cdot\prod_{i\in I}\pi_i'^{m_i}\cdot\prod_{i\in I'}\pi_i^{m_i},$$

$$H_\alpha(n, m_1, \cdots, m_t)$$

$$= \frac{\alpha}{2}\cdot\varepsilon^{n}\cdot\prod_{i\in I}\pi_i^{m_i}\cdot\prod_{i\in I'}\pi_i'^{m_i} + \frac{\alpha'}{2}\cdot\varepsilon'^{n}\cdot\prod_{i\in I}\pi_i'^{m_i}\cdot\prod_{i\in I'}\pi_i^{m_i}.$$

则(7·8)等价于

$$\begin{cases} \pm u = G_\alpha(n, c_1, \cdots, c_t) \\ \pm z = H_\alpha(n, c_1, \cdots, c_t) \end{cases} \tag{7·9}$$

函数 G_α 和 H_α 在假定全部可变但一个固定的意义下是一般递归,则他们变成整双递归序列.

7.4 对于对数线性型

对 $i = 1, \cdots, s$, 我们记 $u_i = \mathrm{ord}_{p_i}(u)$. 设对每个 α,

$$I_U = \{ i \mid 1 \leqslant i \leqslant s, \mathrm{ord}_{p_i}(G_a(n, m_1, \cdots, m_t)) > 0 \text{ 至少对一个 } (n, m_1, \cdots, m_t) \in Z \times N_0^t \text{ 发生} \}.$$

注意因为$(u, y) = 1$，故集 I_U, I, I' 是跳跃的. 我们着手于方程组(7·9)的第一个方程. 写出足够详细的代之

$$\frac{\alpha}{2\sqrt{D}} \cdot \varepsilon^n \cdot \prod_{i \in I} \pi_i^{c_i} \cdot \prod_{i \in I'} \pi_i'^{c_i} - \frac{\alpha'}{2\sqrt{D}} \cdot \varepsilon'^n \cdot \prod_{i \in I} \pi_i'^{c_i} \cdot \prod_{i \in I'} \pi_i^{c_i} = \pm \prod_{i \in I_U} p_i^{u_i}. \tag{7·10}$$

现在，I, I', I_U 依赖于 α，α 依赖于我们预先假定的方程(7·4)的特殊解. 然而，我们知道 α 属于一有限集，可显然易见地计算. 因此，如果对此集的每个 α 我们能完全地解(7·10)，则我们可求出(7·9)的全部解，从而(7·1)也然.

α 的集可简化，不失一般性，如下述. 若 $D \equiv 1 \pmod 8$，则 $b_0 = 0, 1$ 分别对 $\alpha = \alpha_0, 2 \cdot \alpha_0$ 发生. 我们仅需考虑 $2 \cdot \alpha_0$，因为若 $u = u_0, z = z_0$ 是(7·9)关于 $\alpha = \alpha_0$ 的解，则 $u = 2 \cdot u_0, z = 2 \cdot z_0$ 是(7·9)关于 $\alpha = 2 \cdot \alpha_0$ 的解. 因此若 $\alpha = 2 \cdot \alpha_0$ 已经被考虑，就不必要再考虑 $\alpha = \alpha_0$. 同样道理，若 $D \equiv 5 \pmod 8$，则满足 $\alpha = \alpha_0$ 使得 $\mathrm{ord}_2(\alpha_0) = 0$ 也可对 $\alpha = 2 \cdot \alpha_0$ 发生，因此我们仅需考虑后者. 注意现在可出现$(u, y) = 2$. 条件$(u, y) = 1$ 仅用于保证 I_U 和 $I \cup I'$ 是分裂. 这对上述情形满足$(u, y) = 2$ 也仍是正确的. 进而，若$(\alpha_0) \neq (\alpha'_0)$对某 α_0 成立，则我们仅需考虑成对的 α_0, α'_0 中的一个 α. 即是说，若 I, I' 对 α_0 的附属物是 I_0, I_0'，则 I, I' 对 α_0' 的附属物是 I_0', I_0，因此

$$
\begin{aligned}
& G_{\alpha'_0}(n, m_1, \cdots, m_t) \\
& = \frac{\alpha'_0}{2\sqrt{D}} \cdot \varepsilon^n \cdot \prod_{I'_0} \pi_i^{c_i} \cdot \prod_{I_0} \pi'^{c_i}_i - \frac{\alpha_0}{2\sqrt{D}} \cdot \varepsilon'^n \cdot \prod_{I'_0} \pi'^{c_i}_i \cdot \prod_{I_0} \pi_i^{c_i} \\
& = \pm \left[\frac{\alpha'_0}{2\sqrt{D}} \cdot \varepsilon'^{-n} \cdot \prod_{I_0} \pi'^{c_i}_i \cdot \prod_{I'_0} \pi_i^{c_i} - \frac{\alpha_0}{2\sqrt{D}} \cdot \varepsilon^{-n} \cdot \prod_{I_0} \pi_i^{c_i} \cdot \prod_{I'_0} \pi'^{c_i}_i \right] \\
& = \mp G_{\alpha_0}(-n, m_1, \cdots, m_t).
\end{aligned}
$$

(运用 $\varepsilon \cdot \varepsilon' = \pm 1$)，类似地

$$H_{\alpha'_0}(n, m_1, \cdots, m_t) = \pm H_{\alpha_0}(-n, m_1, \cdots, m_t).$$

现在我们由方程(7·10)导出 p－adic 对数线性型，对应于 $i \in I, I'$ 或 I_U，分三种不同形式．令

若 $p_i = 2$，则 $r_i = \frac{3}{2}$；若 $p_i = 3$，则 $r_i = 1$，

若 $p_i \geqslant 5$，则 $r_i = \frac{1}{2}$.

那么 $r_i > 1/(p_i - 1)$，因此若对 $\xi \in K$，$\mathrm{ord}_{p_i}(\xi) \geqslant r_i$，则

$$\mathrm{ord}_{p_i}(\log_{p_i}(1 \pm \xi)) = \mathrm{ord}_{p_i}(\xi). \tag{7·11}$$

现在，我们有下面结果．

引理 7·5　设 $n, c_i (i \in I \cup I')$，$u_i (i \in I_U)$ 满足(7·10)．

(i) 对 $i \in I_U$ 设

$$\lambda_i = \mathrm{ord}_{p_i}(2\sqrt{D}/\alpha'),$$

$$\Lambda_i = \log_{p_i}\left(\frac{\alpha}{\alpha'}\right) + n \cdot \log_{p_i}\left(\frac{\varepsilon}{\varepsilon'}\right) + \sum_{j \in I} c_j \cdot \log_{p_i}\left(\frac{\pi_j}{\pi'_j}\right) - \sum_{j \in I'}$$

$$c_j \cdot \log_{p_i}(\frac{\pi_j}{\pi'_j})$$

若 $u_i + \lambda_l \geqslant r_i$，则

$$u_u + \lambda_i = \mathrm{ord}_{p_i}(\Lambda_i).$$

(ii) 对$i \in I$，设

$$k'_i = \mathrm{ord}_{p_i}(\frac{\alpha'}{\alpha}),$$

$$k_i = \log_{p_i}(\frac{\alpha'}{2\sqrt{D}}) + n \cdot \log_{p_i}(\varepsilon') - \sum_{j \in I_U} u_j \cdot \log_{p_i}(p_j) + \sum_{j \in I} c_j \cdot \log_{p_i}(\pi'_j) + \sum_{j \in I'} c_j \cdot \log_{p_i}(\pi_j).$$

若 $h_i \cdot c_i + k_i \geqslant r_i$，则

$$h_i \cdot c_i + k_i = \mathrm{ord}_{p_i}(k_i).$$

(ii′) 对$i \in I'$，设

$$k'_i = \mathrm{ord}_{p_i}(\frac{\alpha'}{\alpha}),$$

$$k'_i = \log_{p_i}(\frac{\alpha}{2\sqrt{D}}) + n \cdot \log_{p_i}(\varepsilon) - \sum_{j \in I_V} u_j \cdot \log_{p_i}(p_j) + \sum_{j \in I} c_j \cdot \log_{p_i}(\pi_j) + \sum_{j \in I'} c_j \cdot \log_{p_i}(\pi'_j).$$

若 $h_i \cdot c_i + k'_i \geqslant r_i$，则

$$h_i \cdot c_i + k'_i = \mathrm{ord}_{p_i}(k'_i).$$

注：注意上面所有 p－adic 对数是适当定义的，因为其自

变量有 p－adic 次数零．这由事实导出：I_{ii}，I 和 I′是分裂，且若 D≡1(mod 8)来自选择 $\alpha=2\cdot\alpha_0$．

证明：对(i)，(7·10)被其第二项除．对(ii)，(7·10)被其第二项除并加上 1．对(ii′)，(7·10)被其第一项除并加上－1．则在所有三种情形取 p_i－adic 次数，并应用(7·11)．

出现在引理 7·5 中的对数线性型似乎是非齐次的，因为首项系数是 1．然而，将其首项合并到其他项可变为齐次的，如下述．设

$$h^{*}=\mathrm{lcm}(z,h_1,\cdots,h_s).$$

注意由 α 的定义

$$\alpha^{h^{*}}=\pm\varepsilon^{n_0}\cdot\prod_{i\in I}\pi_i^{n_i}\cdot\prod_{i\in I'}\pi'^{n_i}_i\cdot\prod_{i=t+1}^{s}p_i^{n_i}\cdot2^{h^{*}\cdot b_0},\qquad(7\cdot12)$$

这儿指数 n_i 对 $0\leqslant i\leqslant s$ 是整数．这导出

$$\left[\frac{\alpha}{\alpha'}\right]^{h^{*}}=\pm\left[\frac{\varepsilon}{\varepsilon'}\right]^{n_0}\cdot\prod_{i\in I}\left[\frac{\pi}{\pi'}\right]^{n_i}\cdot\prod_{i\in I'}\left[\frac{\pi'}{\pi}\right]^{n_i}.$$

令

$$\Lambda_i^{*}=h^{*}\cdot\Lambda_i,\quad n^{*}=h^{*}\cdot n+n_0,\quad c_j^{*}=h^{*}\cdot c_j+n_j.$$

则得

$$\Lambda_i^{*}=n^{*}\cdot\log_{p_i}\left(\frac{\varepsilon}{\varepsilon'}\right)+\sum_{j\in I}c_j^{*}\cdot\log_{p_i}\left(\frac{\pi_j}{\pi'_j}\right)-$$

$$\sum_{j\in I'} c_j^* \cdot \log_{p_i}\left(\frac{\pi_j}{\pi'_j}\right)$$

注意 D 的素因子正好是分歧素数. 由(7·12),

$$\left(\frac{\alpha}{2\sqrt{D}}\right)^{h^*} = \pm \varepsilon^{n_0} \cdot \prod_{i\in I} \pi_i^{n_i} \cdot \prod_{i\in I'} \pi'^{n_i}_i \cdot \prod_{i=t+1}^{s} p_i^{n_i - v_i} \cdot 2^{h^* \cdot (b_0 - v_0)},$$

其中 $v_i = \frac{1}{2} \cdot h^* \cdot \mathrm{ord}_{p_i}(4D) \in Z, i = t+1, \cdots, s$, 又若 2 分裂, $v_0 = 1$, 其余情形 $v_0 = 0$. 若 $p_i = 2$ 分裂, 我们已假定 $b_0 = 1$. 因此最后的因子变成零. 这样, 设

$$K_i^* = h^* \cdot K_i, K'^*_i = h^* \cdot K'_i, u_j^* = h^* \cdot u_j - (n_j - v_j),$$

$$I_U^* = I_U \cup \{i \mid t+1 \leqslant i \leqslant s, v_i \neq 0\}.$$

则导出

$$K_i^* = n^* \cdot \log_{p_i}(\varepsilon') - \sum_{j\in I_U^*} u_j^* \cdot \log_{p_i}(p_j) + \sum_{j\in I} c_j^* \cdot \log_{p_i}(\pi'_j) + \sum_{j\in I'} c_j^* \cdot \log_{p_i}(\pi_j),$$

$$K'^*_i = n^* \cdot \log_{p_i}(\varepsilon) - \sum_{j\in I_U^*} u_j' \cdot \log_{p_i}(p_j) + \sum_{j\in I} c_j^* \cdot \log_{p_i}(\pi_j) + \sum_{j\in I'} c_j^* \cdot \log_{p_i}(\pi'_j),$$

这导出引理 7·5 的如下改进.

引理 7·6　设 n, c_i 对 $i \in I \cup I'$, u_i 对 $i \in I_U$, 是(7·10)的解, 设 λ_i, k_i, k'_i 如引理 7·5, 又设 h^*, Λ_i^*, K_i^*, K'^*_i, n_i^*, c_i^*,

u_i^*, I_U^* 如上.

(i) 设 $i\in I_U$. 若 $u_i+\lambda_i\geqslant r_i$, 则

$$u_i+\lambda_i+\mathrm{ord}_{p_i}(h^*)=\mathrm{ord}_{p_i}(\Lambda_i^*).$$

(ii) 设 $i\in I$. 若 $h_i\cdot c_i+k_i\geqslant r_i$, 则

$$h_i\cdot c_i+k_i+\mathrm{ord}_{p_i}(h^*)=\mathrm{ord}_{p_i}(k_i^*).$$

(iii) 设 $i\in I'$. 若 $h_i\cdot c_i+k'_i\geqslant r_i$, 则

$$h_i\cdot c_i+k'_i+\mathrm{ord}_{p_i}(h^*)=\mathrm{ord}_{p_i}(k'^*_i).$$

注:我们将研究对变量 n^*, c_i^*, u_i^* 的任意整数值的对数线性型 Λ_i^*, k_i^*, k'^*_i. 注意参数 α 已从这些线性型完全消失. 这意味着我们必须对每一个 D 而不是每个 α 来考虑对数线性型.

7.5 解的上界:概述

首先,我们对于应用 p－adic 对数线性型理论求出出现在线性型中变量 Λ_i^*, k_i^*, k'^*_i 的显示上界,给出一个综合解释. 然后,对于为什么选择这样的方式来应用理论,而不采用其他可能方式,说明我们的理由. 在下节,我们再充分阐述上界的由来. 其结果是用"常数"$C_1, \cdots, C_{12}$来表示,我们说的常数,意指这些数只依赖于(7·10)的参数而不依赖于未知数 n, c_i, u_i.

设

$$M=\max_{i\in I\cup I'}(c_i),\ U=\max_{i\in I_U}(u_i),\ B=\max(M,U,|n|),$$

$$M^*=\max_{i\in I\cup I'}(c_i^*),\ U^*=\max_{i\in I_U}(u_i^*),\ B^*=\max(M^*,U^*,|n^*|),$$

$$N=\max(|n_0|,\cdots,|n_t|,|n_{t+1}-v_{t+1}|,\cdots,|n_s-v_s|),$$

由此导出，对 $X=m,U,B$，有

$$X^*\leqslant h^*\cdot X+N,\quad X\leqslant\frac{X^*+N}{h^*} \qquad (7\cdot13)$$

我们应用引理 2·6 于 p－adic 对数线性型. 考虑到引理 7·6 (i)，对 Λ_i^* 我们发现

$$U<C_1+C_2\cdot\log(B^*), \qquad (7\cdot14)$$

又考虑到引理 7·6(ii)，(ii′)，对 K_i^*，K'^*_i 我们发现

$$M<C_3+C_4\cdot\log(B^*). \qquad (7\cdot15)$$

这里，C_1,C_2,C_3,C_4 是可写出显示式的常数. 为了发现 B 的上界，我们试图找到 C_{10},C_{11}，使

$$B<C_{10}+C_{11}\cdot\log(B^*). \qquad (7\cdot16)$$

考虑到(7·13)，我们随时可以嵌入或删除星号直至不指定常数. 为了证明(7·16)剩下部分，考虑到(7·14)和(7·15)，对界 $|n|$ 用 $\log B$ 的常数倍. 我们要引入某些常数 C_5,C_6,C_7，并区别三种情形：

(a) $-(C_6+C_7\cdot M)\leqslant n\leqslant C_5$,

(b) $n>C_5$,

(c) $n<-(C_6+C_7\cdot M)$ $\qquad (7\cdot17)$

在情形(a)，由(7·15)可知，(7·16)显然成立. 在情形(b)和(c)，G_a 的两项之一处于支配地位. 我们要证明存在常数 C_8, C_9 使得

$$|n| < C_8 + C_9 \cdot U. \tag{7·18}$$

然后由(7·14)导出(7·16).

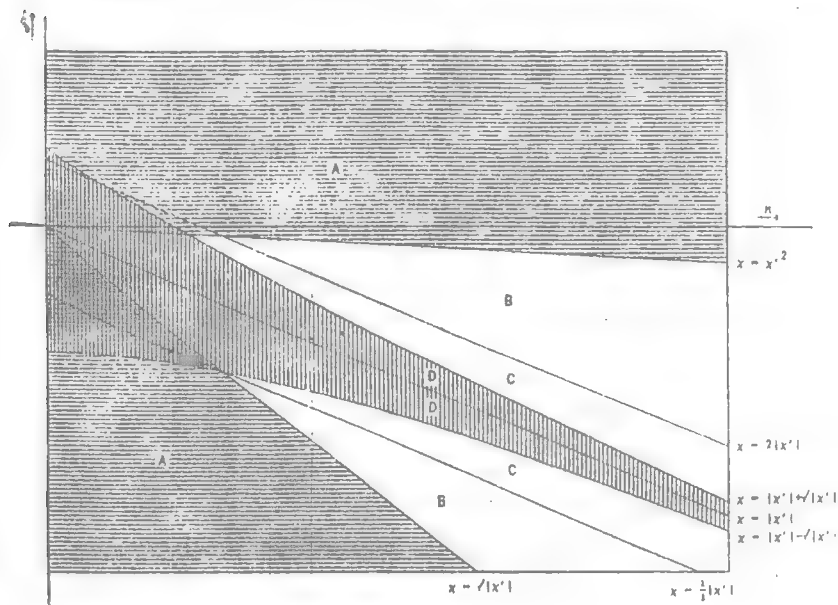
由(7·16)我们直接导出对 B 从而对所有变量复杂的显示上界 C_{12}. 因为常数 $C_1, \cdots, C_4$ 将很大，从而 C_{12} 也将很大. 为了着手找出所有解，要降低这个上界，我们应用 3·11 节所述的，对 p－adic 对数线性型 $\Lambda_i^*, K_i^*, K'^*_i$，应用计算的 p－adic 丢番图逼近方法. 在讨论方法中起决定作用的是常数 $C_5, \cdots, C_9$ 与 $C_1, \cdots, C_4$ 比较，是非常小的. 这一方法导出关于线性型 p－adic 次序的简化上界. 然后我们可以用明显得多的不等式来代替(7·14)和(7·15)，并重复上面的讨论，以找出较之(7·16)明显得多的不等式. 一般我们期待采用此方法可能在一个步骤就把 B 的上界 C_{12} 降低到简化上界 $\log C_{12}$.

在进入详述之前，我们简扼解释一下用实的(代替 p－adic 的)对数线性型理论，随之用实的计算丢番图逼近方法(见 3·7 节)有可能部分地处理(7·10)，以及为什么我们宁可不这样做. 首先，注意到 K_i 和 K'_i 一般比 Λ_i 有更多项，从而处理起来更复杂. 因为 K_i, K'_i 仅在情形(a)出现，这是最困难的情况. 方程(7·10)由三项组成，每一项是纯指数，即其底数固定而指数是可变的. 若这三项中的一项实质上比其它两项小(更特别地，对固定的 $\delta \in (0,1)$，比其它项出现的幂 δ 小)，则我们可应用实方法. 做法有两种. (7·10)写成

$$x - y' = 2 \cdot u \cdot \sqrt{D}.$$

首先假定$|x - x'| < |x'|^{\delta}$.则$|n|$不可能太大,且我们主要的(即有限域除外)对情形(a).遗憾的是这种方法能包括的$|n|$的范围变成小于 M→∞(看下面的例).第二,假定$|x| > |x'|^{1/\delta}$或$|x| < |x'|^{\delta}$.则我们主要对情形(b)或(c).但这一范围用 p－adic 的更容易处理.因为这里我们用线性型Λ_i,而实对数线性型用于此情形一般将有更多的项.给上述范围绘略图,我们应用实理论,将不包含与情形(a)对应的整个区域(看图表 8 中白色的区域).因此我们不能避免使用 p－adic 线性型K_i, K'_i.而避免使用实线性型更方便.

图表 8.



让我们举例说明上述理由. 设 $\alpha=\alpha'=1, \varepsilon=1+\sqrt{2}, \pi_1=1+2\cdot\sqrt{2}, s=1, I=\{1\}, p_1=7, I'=\varnothing, \delta=\frac{1}{2}$, 则有 $x=(1+\sqrt{2})^n\cdot(1+2\cdot\sqrt{2})^M$. 上面给出图表 9 中, (n, M) - 平面的曲线 $x=x'^2, 2\cdot|x'|, |x'|+\sqrt{|x'|}, |x'|, |x'|-\sqrt{|x'|}, \frac{1}{2}\cdot|x'|, \sqrt{|x'|}$ 是四个区域 A, B, C, D 的边界. 有下列可能.

区域	情形 (基本的)	线性型中的项数	
		p - adic 方法	实方法
A	(b), (c)	2	3
B	(b), (c)	2	-
C	(a)	3	-
D	(a)	3	2

最困难部分是 C. 对任意 $c>1, \delta\in(0,1)$, 它可降低到 $\frac{1}{c}\cdot|x'|<x<|x'|-|x'|^{\delta}$ 和 $|x'|+|x'|^{\delta}<x<c\cdot|x'|$, 但将永不消失. 故在情形(a)我们不能避免 p - adic 线性型, 则其一起引进区域 C 和 D.

7.6 解的上界:详述

现在我们着手于前节中步骤概述的充分详述.

我们应用于坤瑞的引理(引理 2·6)如下, 我们有 $L=K=Q(\sqrt{1})$, 因此 $d=2$. 对于 α_i, 我们有 $\varepsilon/\varepsilon', \pi_j/\pi'_j$ 或 $\varepsilon, \varepsilon', p_j, \pi_j, \pi'_j$. 我们计算这些数的高. 立有

$$h(p_j)=\log(p_j), \text{若 } p_j \geqslant 3, h(2)=1,$$

$$h(\varepsilon)=h(\varepsilon')=\frac{1}{2}\cdot\log(\varepsilon),$$

$$h(\pi_j)=h(\pi'_j)=\frac{1}{2}\cdot\log[\max(1,|\pi_j|)\cdot\max(1,|\pi'_j|)].$$

进而，设 $\beta=\varepsilon$ 或 $\beta=\pi_j$. 则导出 β/β' 的系数是 $a_0=|\beta\cdot\beta'|$，我们推断

$$h(\frac{\beta}{\beta'})=\frac{1}{2}\cdot\log[|\beta\cdot\beta'|\cdot\max(1,|\frac{\beta}{\beta'}|)\cdot\max(1,|\frac{\beta'}{\beta}|)]=\log[\max(|\beta|,|\beta'|)].$$

因此

$$h(\frac{\varepsilon}{\varepsilon'})=\log(\varepsilon)$$

$$h(\frac{\pi_j}{\pi'_j})=\log[\max(|\pi_j|,|\pi'_j|)].$$

α_i 的次序的重要性基于两点考虑：它要求 V_i 对 $i=1,\cdots,n-1$ 是依次递增的，而 $\mathrm{ord}_p(b_n)$ 在 $\mathrm{ord}_p(b_i)$ 中是最小的. 因为 b_i 是未知的，我们必须假定 $V_n\leqslant V_1\leqslant\cdots\leqslant V_{n-1}$. 然而在最后的界中仅出现积 $V_1\cdot\cdots\cdot V_n$ 和 V^+_{n-1}. 因此 V_i 的次序仅是定义 V^+_{n-1} 的根据. 此导出了我们可取

$$V_i=\max[h(\alpha_i), f_\wp\cdot(\log p)/d],$$

满足 α_i 的任意次序，若我们定义

$$V_{n-1}^{+}=\max(1, V_1, \cdots, V_n).$$

进而，我们取

$$B=B_0=B_n=B'=\max[|b_1|, \cdots, |b_n|, 2, \frac{4}{3}\cdot n\cdot(p^{f_\lambda/d}-1)].$$

则 $\log(1+\frac{3}{4n}\cdot B)\geqslant f_\lambda\cdot(\log p)/d$. 由 $B\geqslant 2$ 导出 $1+\frac{3}{4n}\cdot B<B$. 因此我们可取

$$W=\log B.$$

有两个另外的条件需检验. 第一个是 $\alpha_1^{b_1}\cdot\cdots\cdot\alpha_n^{b_n}\neq 1$. 若我们假定 b_i 不全为零的明显条件，则上面条件直接得到. 第二个是 $[K(\alpha_1^{1/q}, \cdots, \alpha_n^{1/q}):K]=q^n$，这不那么明显. 对我们的情境，它从下面引理导出. 应用于坤瑞[143]的结果可以避免这样一个条件. 然而，我们这里包括此引理，以说明常常可能证明这个条件，在某情形，它可导出较低的常数.

引理 7·7　设 $K=Q(\sqrt{D})$，满足 ε 作为基本单位，h 作为类数. 设 $p_1, \cdots, p_s$ 是不同素数，又设 μ_i 对于 $i=1, \cdots, s$ 是 K 中属于上列 p_i 的素理想. 设 h_i 是 h 的约数使得 μ_i 是主的，并用 π_i 表示生成元. 设

(1) 所有 p_i 分裂，随之

$$\xi_0=\frac{\varepsilon}{\varepsilon'}, \xi_j=\frac{\pi_j}{\pi'_j}, j=1, \cdots, s;$$

或者

(2) $\xi_0=\varepsilon$ 或 ε'，$\xi_j=\pi_j$ 或 π'_j，$j=1, \cdots, s$.

设 q 是一个奇素数，不整除 h.

那么

$$[K(\xi_0^{1/q},\cdots,\xi_s^{1/q}):K]=q^{s+1}.$$

证明　设 $K_0=K(\xi_0^{1/q})$, $K_i=K_{i-1}(\xi_i^{1/q})$, $i=1,\cdots,s$. 我们对 i 用归纳法来证 $[K_s:K]=q^{s+1}$. 注意 $[K_0:K]=q$. 假定 $[K_i:K]=q^{s+1}$. 要证 $[K_{i+1}:K_i]=q$, 随之, 由于 q 是素数, 便足以证 $\xi_{i+1}\overline{\in}K_i$. 假定结论的反面正确. K_i 是以所有元素

$$\tau_{K_0,\cdots,K_i}=\prod_{j=0}^{i}\xi_j^{K_j/q}$$

为基的 q^{i+1} 维 K－向量空间, 其中 $K_j\in\{0,1,\cdots,q-1\}$, $j=0,\cdots,i$. 由此导出, 存在 $a_{k_0,\cdots,K_i}\in K$, 使得

$$\xi_{i+1}^{1/q}=\sum_{K_0,\cdots,K_i}a_{K_0,\cdots,K_i}\cdot\tau_{K_0,\cdots,K_i}.\tag{7…19}$$

对 $j=0,\cdots,i$, 由 σ_j 生成的 K_i 到 C 的 K－嵌入群定义为

$$\sigma_j(\xi_\iota^{1/q})=\xi_\iota^{1/q},\ \iota=0,\cdots,i,\ \iota\neq j.$$

$$\sigma_j(\xi_j^{1/q})=\rho\cdot\xi_j^{1/q},$$

其中 ρ 是第 q 个本源单位根. 因此, 对 $\iota_j=\{0,1,\cdots,q-1\}$, 所有嵌入由

$$\varphi_{\iota_0,\cdots,\iota_i}=\prod_{j=0}^{i}\sigma_j^{\iota_j}$$

给出. 此导出

$$\varphi_{\iota_0,\cdots,\iota_i}(\tau_{K_0,\cdots,K_i})=\prod_{j=0}^{i}\sigma_j^{\iota_j}[\prod_{m=0}^{i}\xi_m^{k_m/q}]$$

$$=\prod_{j=0}^{i}\rho^{\iota_j\cdot K_j}\cdot\tau_{K_0,\cdots,K_i}=\rho^{\sum_{j=0}^{i}\iota_j\cdot K_j}\cdot\tau_{K_0,\cdots,K_i}.$$

$\xi_{i+1}^{1/q}$在 K 上的最小多项式是 $X^q-\xi_{i+1}$. 因此对于 $j=0,1,\cdots,q-1$, $\xi_{i+1}^{1/q}$的共轭是 $\rho^j\cdot\xi_{i+1}^{1/q}$, 全都具有相同的复合. 存在数 $m_j\in\{0,1,\cdots,q-1\}$使得对 $j=0,1,\cdots q-1$, 有

$$\sigma_j(\xi_{i+1}^{1/q})=\rho^{m_j}\cdot\xi_{i+1}^{1/q}.$$

因此

$$\varphi_{\iota_0,\cdots,\iota_i}(\xi_{i+1}^{1/q})=\rho^{\sum_{j=0}^{i}\iota_j\cdot m_j}\cdot\xi_{i+1}^{1/q}.$$

现在应用 $\varphi_{\iota_0,\cdots,\iota_i}$到(7·19). 则对每一个 tuple$(\iota_0,\cdots,\iota_i)$, 可找到

$$\rho^{\sum_{j=0}^{i}\iota_j\cdot m_j}\cdot\xi_{i+1}^{1/q}=\sum_{K_0,\cdots,K_i}a_{K_0,\cdots,K_i}\cdot\rho^{\sum_{j=0}^{i}\iota_j\cdot k_j}\cdot\tau_{K_0,\cdots,K_i}.$$

这里有含 q^{i+1}个未知数 $a_{K_0,\cdots,K_i}$的 q^{i+1}个线性方程的方程组. 此方程组的行列式恰好是 K 上的判别式 K_i 的平方根, 因此不为零. 因而在 $C^{q^{i+1}}$上恰好在方程组的一个解. 但我们已知解:

$$a_{K_0,\cdots,K_i}=0,\text{若}(K_0,\cdots,K_i)\neq(m_0,\cdots,m_i),$$

$$a_{m_0,\cdots,m_i}=\xi_{i+1}^{1/q}\cdot\tau_{m_0,\cdots,m_i}^{-1}.$$

后一个方程导出 K 上的方程：

$$\xi_{i+1}=a_{m_0,\cdots,m_i}^{q}\cdot\prod_{j=0}^{i}\xi_j^{m_j}.$$

在情形(i)，由此导出理想方程

$$\left[\frac{\mathfrak{p}_{i+1}}{\mathfrak{p}'_{i+1}}\right]^{h_{i+1}}=\mathfrak{a}^q\cdot\prod_{j=1}^{i}\left[\frac{\mathfrak{p}_j}{\mathfrak{p}'_j}\right]^{m_j\cdot h_j},$$

而在情形(ii)，对某分理想 $\mathfrak{a}$(注意$(\xi_0)=(1)$)，得

$$\mathfrak{p}_{i+1}^{(\prime)h_{i+1}}=\mathfrak{a}^q\cdot\prod_{j=1}^{i}\mathfrak{p}_j^{(\prime)m_j\cdot h_j}.$$

(其中 $\mathfrak{p}^{(\prime)}$ 代表 $\mathfrak{p}$ 或 $\mathfrak{p}'$)．因为理想唯一分解，导出对 $j=1,\cdots,i$ 及 h_{i+1}，两情形都有 q 整除所有 $m_j\cdot h_j$．这与假设 $q\nmid h$ 矛盾．

注：1．若 $\mathrm{ord}_p(\alpha_1^{b_1}\cdot\cdots\cdot\alpha_n^{b_n}-1)>1/(p-1)$，则

$$\mathrm{ord}_p(\alpha_1^{b_1}\cdot\cdots\cdot\alpha_n^{b_n}-1)=\mathrm{ord}_p(b_1\cdot\log_p(\alpha_1)+\cdots+b_n\log_p(\alpha_n)).$$

我们宁可用对数变形来做，因为这是我们用于简化上界的一种计算方法．

2．为了应用于坤瑞的引理，我们可取关于 q 的最小奇素数使其不整除 $h\cdot p\cdot(p^{f_{\mathfrak{p}}}-1)$．

现在我们继续计算常数 C_1 和 C_{12}．为了找 C_1 和 C_2，我们对所有 $i\in I_U$，应用引理 2·6 于 Λ_i^*．则我们对每个这样的 i，找到常数 $C_{1,i}$，$C_{2,i}$，使得在条件

$$u_i+\lambda_i\geqslant r_i,\ B^*\geqslant\max[2,\frac{4}{3}\cdot t_i\cdot(p_i^{f_{\lambda i}/2}-1)]$$

之下(其中 t_i 表示 Λ_i' 中项数),我们得到

$$\mathrm{ord}_{\lambda i}(\Lambda_i')<C_{1,i}+C_{2,i}\cdot\log B^*.$$

由引理 7·6(i)及关系 $\mathrm{ord}_{\mathfrak{p}}=e_\lambda\cdot\mathrm{ord}_p$,并假定

$$U\geqslant\max_{i\in I_U}(r_i-\lambda_i),\ B^*\geqslant\max_{i\in I_U}[2,\frac{4}{3}\cdot t_i\cdot(p_i^{f_{\lambda i}/2}-1)],\tag{7·20}$$

我们看出,足以取

$$C_1=\max_{i\in I_U}[-(\lambda_i+\mathrm{ord}_{p_i}(h^*)+C_{1,i}/e_{\lambda i},$$

$$C_2=\max_{i\in I_U}(C_{2,i}/e_{\lambda i});$$

则(7·14)成立.

其次,为得到 C_3 和 C_4,我们分别对所有 $i\in I$ 及 I' 应用引理 2·6 于 K_i' 和 K_i''. 我们用 $X^{(\prime)}$ 表示当 $i\in I$ 时取 X 而当 $i\in I'$ 时取 X'. 由引理 2·6,存在常数 $C_{3,i}$ 和 $C_{4,i}$ 使得在条件

$$h_i\cdot c_i+K_i^{(\prime)}\geqslant r_i,\ B^*\geqslant\max[2,\frac{4}{3}\cdot t_i\cdot(p_i^{f_{\lambda i}/2}-1)]$$

(其中 t_i 也表示 $K_i^{(\prime)*}$ 的项数)之下,导出

$$\mathrm{ord}_{\lambda i}(K_i^{(\prime)*})<C_{3,i}+C_{4,i}\cdot\log B^*.$$

又由引理 7·6(ii),(ii′)导出,在条件

$$M \geqslant \max_{i \in I \cup I'} \left[\frac{r_i - K_i^{(\cdot)}}{h_i} \right], B^* \geqslant \max_{i \in I \cup I'} \left[2, \frac{4}{3} \cdot t_i \cdot (p_i^{f_i/2} - 1) \right] \tag{7·21}$$

之下，足以取

$$C_3 = \max_{i \in I \cup I'} \left[\frac{K_i^{(\cdot)} + \mathrm{ord}_{p_i}(h^*)}{h_i} + \frac{C_{3,i}}{h_i \cdot e_{\mu_i}} \right],$$

$$C_4 = \max_{i \in I \cup I'} \left[\frac{C_{4,i}}{h_i \cdot e_{\mu_i}} \right].$$

则(7·15)成立.

我们取 C_5 和 C_7 如下：

$$C_5 = \log(2 \cdot |\frac{\alpha'}{\alpha}|)/2 \cdot \log \varepsilon,$$

$$C_6 = \log(2 \cdot |\frac{\alpha}{\alpha'}|)/2 \cdot \log \varepsilon,$$

$$C_7 = \left[\sum_{i \in I} \log |\frac{\pi_i}{\pi'_i}| + \sum_{i \in I'} \log |\frac{\pi'_i}{\pi_i}| \right] / 2 \cdot \log \varepsilon.$$

注意 C_5 或 C_6 可以是负的，但总有 $-C_6 < C_5$，进而，C_7 总是严格正的，除非 $I = I' = \varnothing$. 下面说明如何取 C_8 至 C_9. 首先假定

$$n > \max(C_5, 0).$$

那么，由 $\varepsilon \cdot \varepsilon' = \pm 1$ 及选取的 π_i，引用(7·8)得

$$\left|\frac{x}{x'}\right| = \left|\frac{\alpha}{\alpha'}\right| \cdot \left|\frac{\varepsilon}{\varepsilon'}\right|^n \cdot \prod_{i\in I}\left|\frac{\pi_i}{\pi'_i}\right|^{C_i} \cdot \prod_{i\in I'}\left|\frac{\pi'_i}{\pi_i}\right|^{C_i} \geqslant \left|\frac{\alpha}{\alpha'}\right| \cdot \varepsilon^{2\cdot n} > 2,$$

这表明 G_α 的首项处于支配地位. 设

$$p = \prod_{i\in I_U} p_i$$

则导出

$$p^U \geqslant \prod_{i\in I_U} p_i^{u_i} = |x - x'|/2\cdot\sqrt{D} > |x|/4\cdot\sqrt{D}$$

$$= \frac{|\alpha|}{4\sqrt{D}}\cdot\varepsilon^n\cdot\prod_{i\in I}|\pi_i|^{C_i}\cdot\prod_{i\in I'}|\pi'_i|^{C_i} > \frac{|\alpha|}{4\sqrt{D}}\cdot\varepsilon^n,$$

因此

$$n < [\log(\frac{4\sqrt{D}}{|\alpha|}) + U\cdot\log(p)]/\log\varepsilon.$$

其次假定

$$n < \min(-(C_6 + C_7\cdot M), 0)$$

则我们找到 G_α 的第二项处于支配地位, 即

$$\left|\frac{x'}{x}\right| = \left|\frac{\alpha'}{\alpha}\right| \cdot \left|\frac{\varepsilon'}{\varepsilon}\right|^n \cdot \prod_{i\in I}\left|\frac{\pi'_i}{\pi_i}\right|^{C_i} \cdot \prod_{i\in I'}\left|\frac{\pi_i}{\pi'_i}\right|^{C_i}$$

$$\geqslant \left|\frac{\alpha}{\alpha'}\right| \cdot \varepsilon^{-2\cdot n} \cdot \left[\prod_{i\in I}\left|\frac{\pi'_i}{\pi_i}\right| \cdot \prod_{i\in I'}\left|\frac{\pi_i}{\pi'_i}\right|\right]^M$$

$$=\left|\frac{\alpha'}{\alpha}\right|\cdot\varepsilon^{2\cdot(n+C_7\cdot M)}>\left|\frac{\alpha'}{\alpha}\right|\cdot\varepsilon^{2\cdot C_6}=2.$$

令

$$\Gamma=\prod_{i\in I}\min(1,|\pi'_i|)\cdot\prod_{i\in I'}\min(1,|\pi_i|).$$

则导出

$$\begin{aligned}
p^U &\geqslant |x-x'|/2\cdot\sqrt{D}>|x'|/4\cdot\sqrt{D}\\
&=\frac{|\alpha'|}{4\sqrt{D}}\cdot\varepsilon^{|n|}\cdot\prod_{i\in I}|\pi'_i|^{C_i}\cdot\prod_{i\in I'}|\pi_i|^{C_i}\\
&\geqslant\frac{|\alpha|'}{4\sqrt{D}}\cdot\varepsilon^{|n|}\cdot\prod_{i\in I}\min(1,|\pi'_i|)^{C_i}\cdot\prod_{i\in I'}\min(1,|\pi_i|)^{C_i}\\
&\geqslant\frac{|\alpha|'}{4\sqrt{D}}\cdot\varepsilon^{|n|}\cdot\Gamma^M>\frac{|\alpha'|}{4\sqrt{D}}\cdot\varepsilon^{|n|}\cdot\Gamma^{-(|n|-C_6)/C_7}.
\end{aligned}$$

因此

$$|n|<\left[\log\left[\frac{4\sqrt{D}}{|\alpha'|}\cdot\Gamma^{-C_6/C_7}\right]+U\cdot\log(p)\right]/\log[\varepsilon\cdot\Gamma^{1/C_7}].$$

情形(b)和(c)剩下的可能是 $C_5<n\leqslant 0$ 以及 $0\leqslant n<-(C_6+C_7\cdot M)<-C_6$. 注意 $\Gamma\leqslant 1$, 所以可取

$$C_8=\max\left[\log\left[\frac{4\sqrt{D}}{|\alpha|}\right]/\log\varepsilon,\ \log\left[\frac{4\sqrt{D}}{|\alpha'|}\cdot\Gamma^{-C_6/C_7}\right]/\log[\varepsilon\cdot\Gamma^{1/C_7}],\ -C_5,\ -C_6\right]$$

$$C_9 = (\log p)/\log[\varepsilon \cdot \Gamma^{1/C_7}].$$

则在情形(b)和(c),(7·18)成立.现在取

$$C_{10} = \max[C_1, C_3, |C_5|, |C_6| + C_3 \cdot C_7, C_8 + C_1 \cdot C_9],$$

$$C_{11} = \max[C_2, C_4, C_4 \cdot C_7, C_2 \cdot C_9].$$

若条件(7·20)和(7·21)保持,则(7·16)成立.因此由引理 2·1,我们导出下面结果.

引理 7·8 采用上述记号,

$$B^* < C_{12}^*, \quad B < C_{12}$$

无条件成立,其中

$$\begin{aligned} C_{12}^* = \max[&2 \cdot [N + h^* \cdot C_{10} + h^* \cdot C_{11} \cdot \log(h^* \cdot C_{11})], \\ &\max_{i \in I_U}[h^* \cdot (r_i - \lambda_i) + N], \max_{i \in I \cup I'}[h^* \cdot \frac{r_i - k_i^{(')})}{h_i} + N], \\ &2, \max_{i \in I \cup I' \cup I_U}[\frac{4}{3} \cdot t_i \cdot (p_i^{f_i/2} - 1)]] \end{aligned}$$

$$C_{12} = \frac{1}{h^*} \cdot (C_{12}^* + N).$$

证明:显然.

注:1.定理 7·1 是引理 7·8 的直接推论.

2.实际上,C_{12}^*的 max－定义几乎总是首项起支配作用.此外,项 N 的偏离实际上消失.类似地,C_{10}和 C_{11}的定义中,

起支配作用的因子实际上是 C_1 到 C_4.

7.7 简化方法

现在我们想将 B 的上界 C_{12}(或等效的 B^* 的上界 C_{12}^*)降低到小得多的上界.我们运用 3·11 节中所述的 p-adic 计算的丢番图逼近方法.

我们就相关的 i 对 $\Lambda = \Lambda_i^*, K_i^*, K_i''$ 完成这个程序.我们对 p-adic 逼近格 Γ_μ 本身,而不对 3·13 节所述的子格来进来.计算的瓶颈口是对所要求精确度的 p-adic 对数计算以及 L^3-运算的应用.我们涉及到第三章中所详述的.立刻对上述提及的 Λ 找到关于 $\mathrm{ord}_p(\Lambda)$ 的简化上界,我们将这些界与引理 7·6 以及判断(7·13)、(7·17)、(7·17)结合起来以找到 B 和 B^* 的简化界.

当用此方法找到 B, B^* 的简化上界时,我们将 C_{12}, C_{12}^* 用其简化模拟代替,再尝试上述程序.我们可重复论述,只要仍然可得到改进.但在一定阶段,通常接近于实际的最大解,程序将不发生任何进一步改进.随之用某种方法可找到所有解.可采用的方法之一是已在 3·6 节叙述的 Fincke 和 Pohst 运算.另一种方法是在简化界以下直接检验原来丢番图方程的解.对于我们介绍的方程,这种方法将使用同余理论,在得到的界之下找出方程组(7·9)第二个方程的所有解.

7.8 范例

本节对我们的范例$\{p_1, \cdots, p_s\} = \{2, 3, 5, 7\}$,将作出上面

简述的程序，从而验证定理7·2. 在第7·9节表Ⅱ和表Ⅲ，我们给出域$K=Q(\sqrt{D})$上关于D的15个值以及K中因子2,3,5,7的必要数据.

表Ⅱ和表Ⅲ的解释. 对$p_i=2,3,5,7$当$\mathfrak{p}_i$是一个主理想时，我们在表Ⅱ中给出理想$\mathfrak{p}_i$一个生成元满足$\operatorname{ord}_{p_i}(\mathfrak{p}_i)>0$；当$\mathfrak{p}_i$不是主理想时，我们给出"$\mathfrak{p}_i$". 在后面的所有情形，$h_i=2$，因此$\mathfrak{p}_i^2=(\pi_i)$是主的. 星号(*)表示分裂素数. 注意对每个D，素数2,3,5,7至多一个分裂，因此$t\leqslant 1$. 在表Ⅱ最后一列我们对分裂素数p_i给出理想$\mathfrak{p}_i^{h_i}$的生成元π_i. 在表Ⅲ，当$\mathfrak{p}_i$和$\mathfrak{p}_j$不是主的但$\mathfrak{p}_i\cdot\mathfrak{p}_j$是主的，我们给出它一个生成元.

从表Ⅱ和表Ⅲ，容易找到关于I, I'和α的所有可能. 我们可假定$I'=\varnothing$. 在第7·9节表Ⅳ，我们给出所有可能的I, I_U, α（我们给出素数p_i代替指标i）. 当$(\alpha)\neq(\alpha')$时出现星号(*). 集I_U是对所有p_i来检验$G_\alpha(\bmod p_i)$而找到的.

有54种情形满足$I=\varnothing$("对称的"情形)，有54种情形满足$I\neq\varnothing$("非对称的"情形). 我们着手于对称情形. 当素数2,3,5,7中没有一个在$Q(\sqrt{D})$中分裂，结合所有情形，都满足$D=3,5,35,42,210$. 现在$t=0$，因此方程(7·10)变成

$$G_\alpha(n)=\frac{\alpha}{2\sqrt{D}}\cdot\varepsilon^n-\frac{\alpha'}{2\sqrt{D}}\cdot\varepsilon'^n=\pm\prod_{i\in I_U}p_i^{u_i} \qquad (7\cdot 22)$$

满足$A=\varepsilon+\varepsilon'\in Z, B=N_\varepsilon=\varepsilon\cdot\varepsilon'=\pm 1$，对所有$n\in Z$，有

$$G_\alpha(n+2)=A\cdot G_\alpha(n+1)-B\cdot G_\alpha(n).$$

因为$(\alpha)=(\alpha')$，存在一个$n_0\in Z$，使得$\alpha'=\pm\varepsilon^{n_0}\cdot\alpha$. 因此，对所

有 $n \in Z$，

$$|G_a(n_0-n)|=|G_a(n)|,$$

这就解释了为什么称此情形为“对称的”.在这种情况,正如4·5节所说,我们可应用初等同余理论.我们有下面结果.

引理7·9 设$\{p_1,\cdots,p_4\}=\{2,3,5,7\}$.方程(7·1)满足条件(7·2)以及$I=\varnothing$,恰好91个解,出现在第7·9节表Ⅰ中带星号(*)标志的.

概略证明 表V中对这54种情形给出必要的数据.我们解释此表,并留下许多详述给读者检验.对每个$p=2,3,5,7$,给出$\iota_1,n_1,a_1,h_2,\cdots,h_7$.若对$p_x$仅给定$\iota_1$,则对所有$n\in Z$,$p^{\iota_1+1}\nmid G_a(n)$,对至少一个$n\in Z$,$p^{\iota_1}|G_a(n)$.若$n_1,a_1$给定,则

$$p^{\iota_1+1}|G_a(n)\Leftrightarrow n\equiv n_1(\bmod a_1).$$

规定当$n_1=0$时,$n_2=a_1$,当$n_1\neq 0$时,$n_2=n_1$,则n_2是使得$p^{\iota_1+1}|G_a(n_2)$的最小正下标.现在

$$G_a(n_2)|G_a(n),\text{每当 } n\equiv n_1(\bmod a_1),$$

成立.这与双递归序列$\{G_a(n)\}_{n=-\infty}^{\infty}$的对称性质有关.对$q=2,3,5,7$,我们定义了

$$h_q=\operatorname{ord}_q(G_a(n_2)).$$

因此,每当$p^{\iota_1+1}|G_a(n)$,便有$2^{h_2}\cdot 3^{h_3}\cdot 5^{h_5}\cdot 7^{h_7}|G_a(n)$.我们取$\iota_1$大得总有

$$G_\alpha(n_2) > 2^{h_2} \cdot 3^{h_3} \cdot 5^{h_5} \cdot 7^{h_7}.$$

因而,存在某素数 $r \geqslant 11$ 整除 $G_\alpha(n_2)$. 因此 r 整除所有满足 $p^{h_p+1} | G_\alpha(n)$ 的 $G_\alpha(n)$. 由此导出,对方程(7·22)的解,必有用这一方法我们易于找出方程(7·22)的所有解.

让我们用例子 $D=3, \alpha=\sqrt{3}$ 来阐明这一点. 由此

$$G_\alpha(n) = \frac{1}{2} \cdot (2+\sqrt{3})^n + \frac{1}{2} \cdot (2-\sqrt{3})^n,$$

又 $G_\alpha(-n) = G_\alpha(n)$. 对 $G_\alpha(n)$ 我们有:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$G_\alpha(n)$	1	2	7	26	97	362	···				$G_\alpha(14) = 50843527$					
mod4	1	2	−1	2	1	2	−1	2	1	2	−1	2	1	2	−1	2
mod3	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1
mod5	1	2	2	1	2	2	1	2	2	1	2	2	1	2	2	1
mod49	1	2	7	−23	−1	19	−21	−5	1	9	−14	−16	−1	12	0	−12

我们看出,对所有 $n \in Z, 2^2, 3, 5 \nmid G_\alpha(n)$,而 $2 | G_\alpha(n)$ 当且仅当 n 是奇数. 因此 $p=7$ 是唯一引起兴趣的情形. 我们有 $7 | G_\alpha(n)$ 当且仅当 $n \equiv 2 \pmod 4$, $7^2 | G_\alpha(n)$ 当且仅当 $n \equiv 14 \pmod{28}$, (又一般有:当 $k \geqslant 1$,

$$7^K | G_\alpha(n) \Leftrightarrow n \equiv 2 \cdot 7^{K-1} \pmod{4 \cdot 7^{K-1}}$$

又相似的关系对任意对称递归以及任意素数 p 在 $G_\alpha(n)$ 中产生的 p 的任意高次幂都成立,参看引理 4·10). 现在, $\iota_1 = 0$ 导不出(7·23),因为随之 $n=2$, 又 $G_\alpha(2)=7$, 因此没有相宜的

r 存在. 但满足 $t_1=1$, 我们有 $n_2=14$ 及 $h_2=h_3=h_5=0$, $h_7=0$, (7·23)成立, 因为 $G_\alpha(14)>7^2$. 因此存在素数 $r\geqslant 11$ 使得 $r \mid G_\alpha(14)$, 因此, 每当 $7^2 \mid G_\alpha(n)$, 就有 $r \mid G_\alpha(n)$. 由此导出对(7·22)的解, 有 $G_\alpha(n)\leqslant 2^1\cdot 3^0\cdot 5^0\cdot 7^1=14$, 因此由上表可列出所有解. 注意 r 明晰地知道并不是必要的, 仅在 $G_\alpha(n_2)$ 足够大时. 在我们的例中, $r=337$ 或 $r=3079$ 满足.

最后, 我们对待剩下的 54 种情形, 其中 $I\neq\varnothing$. 此时我们需要 7·5 到 7·7 节所述的非初等简化方法.

在我们所有的例中, 集 I 仅包含一个元素, 因为仅存在一个分裂素数. 我们用 π 表示 π_i 属于这一素数, c_i 写成 m. 方程(7·10)现在写成

$$\frac{\alpha}{2\cdot\sqrt{D}}\cdot\varepsilon^n\cdot\pi^m-\frac{\alpha'}{2\cdot\sqrt{D}}\cdot\varepsilon'^n\cdot\pi'^m=\pm\prod_{j\in I_U}p_j^{u_j}.$$

根据 7·6 节, 对 54 种情形中每种情形, 我们计算常数 C_1 到 C_{12}, C_{12}^*. 我们删除这些计算的详述, 简单地在第 7·9 节表 Ⅵ 中给出数据. 在表中我们对每一个 D 给出 $p_i\in I_U$ 连同 ν_i 和 λ_i (其结果是 λ_i 不依赖于 α, 仅依赖于 p_i). 值"$n_\varepsilon, n_\pi, n_2, n_3, n_5, n_7$"是整数, 使得

$$\alpha^2=\pm\varepsilon^{n_\varepsilon}\cdot\pi^{n_\pi}\cdot 2^{n_2}\cdot\cdots\cdot 7^{n_7}.$$

由此导出在所有情形都有 $C_{12}^*<3.23\times 10^{30}$.

下一步是定义格, 并找出格中最短非零向量的下界. 我们着手对待 Λ_i^*, 其中对 10 个 D 的每一个有 3 个值. 我们计算

出

$$\theta = -\frac{\log_{p_i}\left[\frac{\pi}{\pi'}\right]}{\log_{p_i}\left[\frac{\varepsilon}{\varepsilon'}\right]} \text{ 或 } -\frac{\log_{p_i}\left[\frac{\varepsilon}{\varepsilon'}\right]}{\log_{p_i}\left[\frac{\pi}{\pi'}\right]}$$

的 30 个值，使得它们是对要求精度的 μ 数字的 p_i - adic 整数．我们取 μ 如下：

p_i	μ	p_i^μ
2	209	8.22×10^{62}
3	133	2.87×10^{63}
5	95	2.52×10^{66}
7	76	1.69×10^{64}

为了使 p_i^μ 稍微大于最大值 C_{12}^{*2}，就是 1.05×10^{61}．我们计算 $\theta^{(\mu)}$ 的 30 个值，但这里不给出．格 Γ_μ 由矩阵

$$\begin{bmatrix} 1 & 0 \\ \theta^{(\mu)} & p^\mu \end{bmatrix}$$

的列向量生成．对这 30 个格的每一个，我们完成 3·10 中的 p - adic 连分数运算．在下表中，对每个 D 我们给出最大值 C_{12}^*（对每个 α，存在着一个对应值）以及找到的 $\iota(\Gamma_\mu)$ 的最小界（每个 $i\in I_U$ 对应一个）．我们删去进一步的详述．

D	p	μ_0	$C^*_{12}\leqslant$	$\iota(\Gamma_\mu)>$	$U\leqslant$
2	2,3,5	1.5,1.0,1.0	$3.19\times10^{[illegible]}$	8.26×10^{30}	210
6	2,3,7	1.5,1.5,1.0	2.72×10^{26}	2.05×10^{31}	210
7	2,5,7	2.0,1.0,0.5	1.07×10^{30}	2.43×10^{31}	210
10	2,5,7	1.5,0.5,1.0	$3.22\times10^{[illegible]}$	$2.[illegible]\times10^{31}$	210
14	2,3,7	1.5,1.0,0.5	4.80×10^{26}	1.48×10^{31}	210
15	2,3,5	3.5,1.5,0.5	2.15×10^{28}	1.55×10^{31}	212
21	2,3,7	3.0,0.5,0.5	1.90×10^{26}	7.78×10^{30}	211
30	2,3,5	2.5,0.5,0.5	4.15×10^{28}	1.37×10^{31}	211
70	2,5,7	2.5,0.5,0.5	3.23×10^{30}	2.51×10^{31}	211
105	3,5,7	1.5,0.5,0.5	4.54×10^{29}	3.96×10^{31}	134

在所有情形，$\iota(\Gamma_\mu)>\sqrt{2}\cdot C^*_{12}$. 因此，对 $n=2, c_1=0, c_2=1$，由引理 3·14 导出

$$\mathrm{ord}_{p_i}(\Lambda_i^*)<\mu+\mu_0,\ i\in I_U,$$

其中

$$\mu_0=\min\left[\mathrm{ord}_{p_i}\left(\log_{p_i}\left(\frac{\varepsilon}{\varepsilon'}\right)\right),\ \mathrm{ord}_{p_i}\left(\log_{p_i}\left(\frac{\pi}{\pi'}\right)\right)\right],$$

如上面给出的. 由 $\lambda_i+\mathrm{ord}_{p_i}(h^*)\geqslant0$，根据引理 7·6(i) 我们得到关于 $u_i, i\in I_U$ 的上界，因此 U 的上界如上面所给.

其次，我们处理 K_i^*，对每个 D，一个 K_i^* 有 5 项，即

$$K_i^*=n^*\cdot\log_{p_i}(\varepsilon')+m^*\cdot\log_{p_i}(\pi')-\sum_{\substack{1\leq j\leq 4\\ j\neq i}}u_j^*\cdot\log_{p_i}(p_j),$$

其中 $i\in I$，因此 p_i 是分裂素数. 我们有下面数据

D	p_i	$\sqrt{D}(\bmod\ p_i)$	$\mathrm{ord}_{p_i}(\log_{p_i}(\cdot))$					
			ε'	π'	2	3	5	7
2	7	3	1	2	1	1	1	–
6	5	4	1	1	1	1	–	2
7	3	1	1	1	1	–	1	1
10	3	2	1	1	1	–	1	1
14	5	2	1	1	1	1	–	2
15	7	6	1	1	1	1	1	–
21	5	4	1	1	1	1	–	2
30	7	4	1	1	1	1	1	–
70	3	2	1	1	1	–	1	1
105	2	1 (mod 4)	2	4	–	2	2	3

由此表,对$\sqrt{D}(\bmod p_i)$的选取变得明显了.由此导出$\mathrm{ord}_{p_i}(\log_{p_i}(\varepsilon'))$总是上表中5个$\mathrm{ord}_{p_i}$的最小一个.因此我们定义:

$$\theta_i=-\frac{\log_{p_i}(\pi')}{\log_{p_i}(\varepsilon')},\theta_{2,3,4}=-\frac{\log_{p_i}(p_j)}{\log_{p_i}(\varepsilon')},(j\in\{1,2,3,4\},j\neq i),$$

我们计算适于μ数字的这些数,连同μ如下:

p_i	μ	p_i^{μ}
2	539	1.80×10^{162}
3	343	4.49×10^{163}
5	245	1.77×10^{171}
7	196	4.36×10^{165}

因此p_i^{μ}稍微大于最大的C_{12}^{*5}.我们计算$\theta_{1,2,3,4}^{(\mu)}$的40个值,但这里不给出.格Γ_{μ}由下列矩阵

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \theta_1^{(\mu)} & \theta_2^{(\mu)} & \theta_3^{(\mu)} & \theta_4^{(\mu)} & p^{\mu} \end{bmatrix}.$$

的列生成.我们用 L^3－运算计算 10 个格的简化基.我们删去计算的详述.我们找到的数据如下：

D	p in I	μ	μ_0	$C_{12}^* \leqslant$	$\iota(\Gamma_\mu) >$	$M \leqslant$
2	7	196	1	3.19×10^{28}	2.25×10^{32}	196
6	5	245	1	2.72×10^{26}	2.16×10^{33}	245
7	3	343	1	1.07×10^{30}	1.14×10^{32}	343
10	3	343	1	3.22×10^{29}	1.07×10^{32}	343
14	5	245	1	4.80×10^{26}	4.92×10^{33}	245
15	7	196	1	2.15×10^{28}	2.78×10^{32}	196
21	5	245	1	1.90×10^{26}	4.37×10^{33}	245
30	7	196	1	4.15×10^{28}	2.69×10^{32}	196
70	3	343	1	3.23×10^{30}	1.03×10^{32}	343
105	2	539	2	4.54×10^{29}	6.68×10^{31}	540

所有例子中，$\iota(\Gamma_\mu)>\sqrt{5}\cdot C_{12}^*$，因此，由引理 3·14 及 7·6(ii)，由 $K_i+\mathrm{ord}_{p_i}(h^*)\geqslant0$ 及 $h_i\geqslant1$，我们有 $M\leqslant\mathrm{ord}_{p_i}(K_i^*)<\mu+\mu_0$，因此 M 的上界如同在上表中给出的.

最后，我们对 $|n|$ 从而对 B 计算新的简化上界，由

$$|n| < \max[C_5, C_6 + C_7 \cdot M, C_8 + C_9 \cdot U],$$

我们找到数据如下表.

D	$C_5<$	$C_6<$	$C_7<$	$C_8<$	$C_9<$	$M\leqslant$	$U\leqslant$	$\|n\|\leqslant$	$B\leqslant$	$N\leqslant$	$B^*\leqslant$
2	0.394	0.394	0.420	1.967	3.859	196	210	812	812	3	1627
6	0.152	0.652	0.190	1.345	1.631	245	210	343	343	3	689
7	0.126	0.626	0.357	2.702	2.757	343	210	581	581	2	1164
10	0.601	0.191	0.181	1.396	2.337	343	210	492	492	3	987
14	0.102	0.602	0.325	1.861	1.508	245	210	318	318	3	639
15	0.540	0.668	0.257	1.394	1.649	196	212	350	350	2	702
21	0.222	0.722	0.142	1.564	2.386	245	211	505	505	1	1011
30	0.414	0.613	0.399	1.239	1.102	196	211	233	233	3	469
70	0.362	0.556	0.390	2.729	1.505	343	211	320	343	3	689
105	0.390	0.579	0.379	3.232	2.545	540	134	344	540	1	1081

这里我们运用 $B^* \leqslant h^* \cdot B + N$ 及 $h^* = 2$. 因此, 第一步得到界 $B^* < 3.23 \times 10^{30}$ 到 $B^* \leqslant 1627$. 总的计算时间是 1715 秒, 其中每一个 2 维格平均 0.7 秒, 而每一个 5 维格 170 秒.

我们进行进一步的简化步骤, 现在用上面给出的 B^* 的简化界代替 C_{12}. 我们给出 A_i^* 的数据如下表. 对 μ 我们取 $\mu_1 \cdot \mu_2$, 连同 μ_1, μ_2 如下:

P	2	3	5	7
μ_2	11	7	5	4

D	$B^* \leqslant$	$B \leqslant$	$M \leqslant$	$\mu \leqslant$	$\chi(\Gamma_\mu) \geqslant$	[illegible]	$U \leqslant$
2	1627	2301	2	22	1.82×10^3	1.5	23
6	689	975	3	33	3.99×10^4	1.5	34
7	1164	1646	3	33	4.50×10^4	2.0	34
10	987	1396	3	33	5.91×10^4	1.5	34
14	639	904	3	33	2.58×10^4	1.5	34
15	702	993	3	33	7.36×10^4	3.5	36
21	1011	1430	3	33	2.00×10^4	3.0	35
30	469	664	2	22	9.98×10^2	2.5	24
70	689	975	3	33	5.76×10^4	2.5	35
105	1081	1529	3	21	3.89×10^4	1.5	22

我们找到 $\varepsilon(\Gamma_\mu)$ 及 U 的界如上表所给出的. 对于 [illegible] 我们发现, 由于 $\mu=\mu_1\mu_2$, 关于 μ_2 如上述, 而 μ_1 如下表所列, 结果在表中给出.

D	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
2	1627	[illegible]	[illegible]	[illegible]	[illegible]	1	28	90	90	183
6	689	[illegible]	[illegible]	30	4.04×10^3	1	30	145	145	293
7	1164	2603	7	49	1.07×10^4	1	49	96	96	194
10	987	2207	7	49	1.16×10^4	1	49	80	80	163
14	639	1429	6	30	3.07×10^3	1	30	53	53	109
15	702	1570	6	24	2.70×10^3	1	24	60	60	122
21	1011	2261	6	30	3.88×10^3	1	30	85	[illegible]	171
30	469	1049	6	24	2.50×10^3	1	24	27	[illegible]	57
70	689	1541	6	42	1.90×10^3	1	42	55	55	113
105	1081	2418	7	77	1.00×10^4	2	78	59	78	157

计算时间为 15 秒.

我们进行第三步, 并仿照上面给出 Λ_i^* 的数据:

D	$B^* \leqslant$	$\sqrt{2} \cdot B^* <$	μ_1	$\mu \leqslant$	$\iota(\Gamma_\mu) \geqslant$	$\mu_0 \leqslant$	$U \leqslant$
2	183	258.9	2	22	1821	1.5	23
6	299	414.4	2	22	875	1.5	23
7	194	274.4	2	22	1285	2	23
10	163	230.6	2	22	634	1.5	23
14	109	154.2	2	22	268	1.5	23
15	122	172.6	2	22	873	3.5	25
21*	171	241.9	2	22	818	3	25
30	57	80.7	2	22	998	2.5	24
70	113	159.9	2	22	585	2.5	24
105	157	222.1	2	14	281	1.5	15

又对 K_i^* 给出数据：

D	$B^* \leqslant$	$\sqrt{5} \cdot B^* <$	μ_1	$\mu \leqslant$	$\iota(\Gamma_\mu) \geqslant$	$\mu_0 \leqslant$	$M \leqslant$
2	183	409.3	5	20	440	1	20
6	293	655.2	5	25	665	1	25
7	194	433.8	6	42	602	1	42
10	163	364.5	5	35	473	1	35
14	109	243.8	5	25	626	1	25
15	122	272.9	6	24	2700	1	24
21	171	382.4	5	25	645	1	25
30	57	127.5	4	16	129	1	16
70	113	252.7	5	35	366	1	35
105	157	351.1	5	55	354	2	56

最后，对$|n|$，进而当$i\in I_U$时，对$\mathrm{ord}_{p_i}(u)$给出更详细数据.

D	$M\leqslant$	$u_2\leqslant$	$u_3\leqslant$	$u_5\leqslant$	$u_7\leqslant$	$\|n\|\leqslant$
2	20	23	14	10	0	90
6	25	23	15	0	8	38
7	42	23	0	10	8	66
10	35	23	0	10	8	55
14	25	23	14	0	8	36
15	24	25	15	10	0	42
21	25	24	14	0	8	61
30	16	24	14	10	0	27
70	35	24	0	10	8	65
105	56	0	14	10	8	41

现在，如果我们继续用同样方法，将得不到任何进一步改进. 但现在上界已小得足以容许列举剩下的可能，可用 mod p 对 p=2,3,5,7 计算. 这样做，找到剩下的解在表 I 中呈现. 最后这一步，我们仅用 3 秒计算机时间.

定理 7·2 证毕.

7.9. 表.

Table I. (Theorem 7.2)

Nr	X	Y	Z	D
1	4375	-4374	1	7
2	2401	-2400	1	1
3	225	-224	1	1
4	126	-125	1	14
5	81	-80	1	1
6	64	-63	1	1
7	50	-49	1	2
8	49	-48	1	1
9	36	-35	1	1
10	28	-27	1	7
11	25	-24	1	1
12	21	-20	1	21
13	16	-15	1	1
14	15	-14	1	15
15	10	-9	1	10
16	9	-8	1	1
17	8	-7	1	2
18	7	6	1	7
19	6	-5	1	6
20	5	-4	1	5
21	4	-3	1	1
22	3	-2	1	3
23	2	-1	1	2
24	490	-486	2	10
25	54	-50	2	6
26	49	-45	2	1
27	25	21	2	1
28	18	-14	2	2
29	14	-10	2	14
30	10	-6	2	10
31	9	-5	2	1
32	7	-3	2	7
33	6	-2	2	6
34	5	-1	2	5
35	3	1	2	3
36	2	2	2	2
37	384	375	3	6
38	105	-96	3	105
39	84	-75	3	21
40	49	-40	3	1
41	30	-21	3	30
42	25	-16	3	1
43	24	-15	3	6
44	21	-12	3	21
45	16	-7	3	1
46	15	-6	3	15
47	14	5	3	14
48	12	-3	3	3
49	10	-1	3	10
50	6	1	3	2
51	7	2	3	7
52	6	3	3	6
53	5	4	3	5
54	70	-54	4	70
55	30	-14	4	30
56	25	-9	4	1
57	21	5	4	21
58	18	-2	4	2
59	15	1	4	15
60	14	2	4	14
61	10	6	4	10
62	9	7	4	1
63	5145	-5120	5	105
64	270	-245	5	30
65	160	-135	5	10
66	105	-80	5	105
67	81	-56	5	1
68	70	-45	5	70
69	60	-35	5	15
70	49	-24	5	1
71	45	-20	5	5
72	40	-15	5	10
73	35	-10	5	35
74	32	-7	5	2
75	30	-5	5	30
76	28	-3	5	7
77	27	-2	5	3
78	24	1	5	6
79	21	4	5	21
80	20	5	5	5
81	18	7	5	2
82	16	9	5	1
83	15	10	5	15
84	50	-14	6	2
85	42	-6	6	42
86	35	1	6	35
87	30	6	6	30
88	21	15	6	21
89	1750	-1701	7	70
90	945	-896	7	105
91	625	-576	7	1
92	224	-175	7	14
93	189	-140	7	21

Nr	X	Y	Z	D
94	175	- 126	7	7
95	112	- 63	7	7
96	105	56	7	105
97	84	- 35	7	21
98	81	32	7	1
99	70	- 21	7	70
100	66	- 25	7	1
101	63	- 14	7	7
102	56	- 7	7	14
103	54	- 5	7	6
104	50	- 1	7	2
105	48	1	7	3
106	45	4	7	5
107	42	7	7	42
108	40	9	7	10
109	35	14	7	35
110	28	21	7	7
111	25	24	7	1
112	750	- 686	8	30
113	189	- 125	8	21
114	162	- 98	8	2
115	70	- 6	8	70
116	63	1	8	7
117	54	10	8	6
118	50	14	8	2
119	49	15	8	1
120	375	- 294	9	15
121	256	- 175	9	1
122	105	- 24	9	105
123	96	- 15	9	6
124	84	- 3	9	21
125	80	1	9	5
126	75	6	9	3
127	60	21	9	15
128	56	25	9	14
129	49	32	9	1
130	343	243	10	7
131	135	- 35	10	15
132	105	5	10	105
133	98	2	10	2
134	90	10	10	10
135	70	30	10	70
136	625	- 504	11	1
137	441	- 320	11	1
138	256	- 135	11	1
139	196	- 75	11	1
140	175	54	11	7
141	135	- 14	11	15
142	128	- 7	11	2
143	126	- 5	11	14
144	125	- 4	11	5
145	120	1	11	30
146	112	9	11	7
147	105	16	11	105
148	100	21	11	1
149	96	25	11	6
150	81	40	11	1
151	72	49	11	2
152	294	150	12	6
153	150	- 6	12	6
154	147	- 3	12	3
155	729	- 560	13	1
156	512	343	13	2
157	294	- 125	13	6
158	250	81	13	10
159	225	- 56	13	1
160	196	27	13	1
161	189	20	13	21
162	175	- 6	13	7
163	168	1	13	42
164	162	7	13	2
165	160	9	13	10
166	144	25	13	1
167	120	49	13	30
168	105	64	13	105
169	250	- 54	14	10
170	210	14	14	210
171	189	7	14	21
172	175	21	14	7
173	126	70	14	14
174	960	735	15	15
175	245	- 20	15	5
176	240	- 15	15	15
177	224	1	15	14
178	210	15	15	210
179	120	105	15	30
180	270	14	16	30
181	250	6	16	10
182	175	81	16	7
183	6561	6272	17	1
184	1024	- 735	17	1
185	625	336	17	1
186	343	- 54	17	7
187	324	- 35	17	1
188	294	- 5	17	6
189	288	1	17	2
190	280	9	17	70
191	240	49	17	15
192	225	64	17	1
193	189	100	17	21

Nr	X	Y	Z	D
194	294	96	18	6
195	1225	-864	19	[illegible]
196	486	-125	19	6
197	441	480	19	[illegible]
198	574	-204	19	15
199	360	220	19	10
200	343	248	19	[illegible]
201	988	29	19	21
202	280	[illegible]	19	70
203	256	800	19	[illegible]
204	490	98	20	10
205	400	61	20	5
206	525	-84	21	21
207	448	77	21	7
208	420	21	21	105
209	306	105	21	21
210	729	245	22	[illegible]
211	490	-61	22	10
212	486	-2	22	6
213	1215	686	23	15
214	1029	-500	23	21
215	729	200	23	1
216	928	-96	23	1
217	925	4	23	21
218	504	25	23	14
219	480	49	23	30
220	448	81	23	7
221	625	-49	24	1
222	945	320	25	105
223	640	-15	25	10
224	630	-5	25	70
225	576	49	25	1
226	490	135	25	10
227	686	-10	26	14
228	675	1	26	3
229	1029	300	27	21
230	750	2	27	30
231	735	-6	27	15
232	1134	350	28	14
233	1225	384	29	1
234	640	1	29	210
235	729	112	29	1
236	625	216	29	1
237	441	400	29	1
238	6561	5600	31	1
239	2401	1440	31	1
240	1024	-63	31	1
241	760	1	31	15
242	945	16	31	105
243	625	336	31	1
244	1029	[illegible]	32	21
245	2625	-1936	33	105
246	1029	260	33	21
247	1701	-560	35	2
248	1260	-99	35	35
249	1215	20	35	5
250	1120	105	35	[illegible]
251	988	280	35	105
252	1102	[illegible]	37	2
253	1344	1080	37	21
254	1225	144	37	1
255	729	640	37	1
256	1468	-144	38	2
257	1536	-205	39	6
258	1500	21	39	15
259	896	625	39	14
260	2401	-720	41	1
261	1701	-20	41	21
262	1680	1	41	105
263	1600	81	41	1
264	1750	14	42	70
265	1800	49	43	2
266	1120	729	43	70
267	1250	686	44	2
268	1920	105	45	30
269	16384	-14175	47	1
270	2401	-192	47	1
271	2205	4	47	5
272	2160	49	47	15
273	2625	-224	49	105
274	2400	-1	49	6
275	1701	700	49	21
276	2430	-70	50	30
277	2625	-24	51	105
278	2401	200	51	1
279	15309	-12500	53	21
280	2800	-9	53	7
281	2025	784	53	1
282	3430	-405	55	70
283	3024	1	55	21
284	3150	-14	56	14
285	3200	49	57	2
286	4050	-686	58	2
287	3456	25	59	6
288	2401	1080	59	1
289	35721	-32000	61	1
290	4096	-375	61	1
291	3969	-125	62	1
292	2625	1344	63	105
293	3969	256	65	1

Nr	X	Y	Z	D
294	4480	9	67	70
295	4374	250	68	6
296	5145	- 384	69	105
297	15625	- 10584	71	1
298	5040	1	71	35
299	4096	945	71	1
300	4704	625	73	6
301	5145	480	75	105
302	3375	2401	76	15
303	6804	- 875	77	21
304	6561	- 320	79	1
305	6250	- 9	79	10
306	3840	2401	79	15
307	8505	- 1280	85	105
308	7840	81	89	10
309	65625	- 57344	91	105
310	8505	- 224	91	105
311	10240	- 1215	95	10
312	9402	1	97	3
313	9800	1	99	2
314	10200	- 5	101	14
315	9375	1029	102	15
316	10584	25	103	6
317	11250	- 14	106	2
318	12544	225	113	1
319	10368	2401	113	2
320	13236	- 5	115	30
321	15625	1701	118	1
322	14336	- 175	119	14
323	14175	- 14	119	7
324	14406	- 6	120	6
325	18225	- 3584	121	1
326	16128	1	127	7
327	15625	504	127	1
328	15625	1536	131	1
329	17500	189	133	7
330	18144	625	137	14
331	18730	294	138	30
332	117649	- 97200	143	1
333	21504	105	147	21
334	24010	15	155	10
335	23625	1024	157	105
336	25920	1	161	5
337	26250	- 6	162	42
338	16807	13122	173	7
339	30618	7	175	42
340	32768	- 7	181	2
341	33614	- 125	183	14
342	43740	- 1715	205	15
343	43750	- 486	208	70
344	46305	- 80	215	105
345	50625	- 896	223	1
346	49000	729	223	10
347	129654	- 78125	227	6
348	55566	- 3125	229	14
349	60025	- 1944	241	1
350	59535	1	244	15
351	59049	1960	247	1
352	63000	1	251	70
353	[illegible]4000	9	253	10
354	48384	15625	253	21
355	59049	7000	257	1
356	69120	49	263	30
357	85750	- 486	292	70
358	83349	2500	293	21
359	140625	- 43904	311	1
360	109375	- 1134	329	7
361	82944	30625	337	1
362	128625	256	359	105
363	137781	- 140	371	21
364	76545	71680	385	105
365	196830	- 33614	404	30
366	117649	48000	407	1
367	168070	30	410	70
368	179200	6561	431	7
369	137200	59049	443	7
370	201684	- 1875	447	21
371	201600	1	449	14
372	214375	- 6	463	7
373	252105	24576	477	105
374	243000	49	493	30
375	245760	- 735	495	15
376	262144	- 5145	517	1
377	390625	- 112896	527	1
378	688905	- 5	830	105
379	1058841	- 20480	1019	1
380	1440000	2401	1201	1
381	1640625	336	1281	105
382	4214784	25	2053	21
383	4782969	4375	2188	1
384	5764801	- 9600	2399	1
385	19140625	- 17496	4373	1
386	23049600	1	4801	6
387	76545000	1	8749	42
388	199290375	- 686	14117	15

Table II.

D	h	ε	[illegible]	p_1	p_2	p_3	p_4	[illegible]
2	1	$1+\sqrt{2}$	[illegible]	$\sqrt{2}$	3	5	$1+2\sqrt{2}$	$1+2\sqrt{2}$
3	1	$2+\sqrt{3}$	[illegible]	$1+\sqrt{3}$	$\sqrt{3}$	5	[illegible]	
5	1	$\frac{1}{2}(1+\sqrt{5})$	[illegible]	2	3	$\sqrt{5}$	[illegible]	
6	1	$5+2\sqrt{6}$	[illegible]	$2+\sqrt{6}$	$3+\sqrt{6}$	$1+\sqrt{6}$	[illegible]	$1+\sqrt{6}$
7	1	$8+3\sqrt{7}$	1	$3+\sqrt{7}$	$2+\sqrt{7}$	5	$\sqrt{7}$	$2+\sqrt{7}$
10	2	$3+\sqrt{10}$	-1	p_1	p_2	p_3	7	$1+\sqrt{10}$
14	1	$15+4\sqrt{14}$	1	$4+\sqrt{14}$	3	$3+\sqrt{14}$	$7+2\sqrt{14}$	$5+\sqrt{14}$
15	2	$4+\sqrt{15}$	1	p_1	p_2	p_3	p_4	[illegible] $+\sqrt{15}$
21	1	$\frac{1}{2}(5+\sqrt{21})$	1	2	$\frac{1}{2}(3+\sqrt{21})$	$\frac{1}{2}(1+\sqrt{21})$	$\frac{1}{2}(7+\sqrt{21})$	$\frac{1}{2}(1-\sqrt{21})$
30	2	$11+2\sqrt{30}$	1	p_1	p_2	$5+\sqrt{30}$	p_4	$13+2\sqrt{30}$
35	2	$6+\sqrt{35}$	1	p_1	3	p_3	p_4	
42	2	$13+2\sqrt{42}$	1	p_1	p_2	5	$7+\sqrt{42}$	
70	2	$251+30\sqrt{70}$	1	p_1	p_2^*	$25+3\sqrt{70}$	p_4	$17+2\sqrt{70}$
105	2	$41+4\sqrt{105}$	1	p_1^*	p_2	$10+\sqrt{105}$	p_4	$\frac{1}{2}$([illegible] $-\sqrt{105}$)
210	4	$29+2\sqrt{210}$	1	p_1	p_2	p_3	p_4	

D	$p_1 \cdot p_2$	$p_1 \cdot p_3$	$p_1 \cdot p_4$	$p_2 \cdot p_3$	$p_2 \cdot p_4$	$p_3 \cdot p_4$
10	$-2+\sqrt{10}$	$\sqrt{10}$		$5-\sqrt{10}$		
15	$3+\sqrt{15}$	$5+\sqrt{15}$	$1+\sqrt{15}$	$\sqrt{15}$	$6+\sqrt{15}$	$5+2\sqrt{15}$
30	$6+\sqrt{30}$	–	$4+\sqrt{30}$	–	$3+\sqrt{30}$	
35	–	$5+\sqrt{35}$	$7+\sqrt{35}$			$\sqrt{35}$
42	$6+\sqrt{42}$	–	–	–		
70	$-8+\sqrt{70}$		$42+5\sqrt{70}$		$7+\sqrt{70}$	
105	$\frac{1}{2}(-9+\sqrt{105})$		$\frac{1}{2}(17+\sqrt{105})$		$21+2\sqrt{105}$	
210	–		$14+\sqrt{210}$	$15+\sqrt{210}$		

Table IV.

D	α	j	I_U	D	α	j	I_U
2	1	–	2357	10	1	-	2357
	1	7	235		1	3	2 57
	$\sqrt{2}$		3 7		$\sqrt{10}$	-	3 7
	$\sqrt{2}$	7	35		$\sqrt{10}$	3	7
3	1		2357		$-2+\sqrt{10}$	3	57
	$\sqrt{3}$	-	2 7		$5-\sqrt{10}$	3	2 7
	$1+\sqrt{3}$	-	3	14	1	–	2357
	$3+\sqrt{3}$		5		1	5	23 7
5	2	-	2357		$\sqrt{14}$		35
	$2\sqrt{5}$		23 7		$\sqrt{14}$	5	3
6	1		2357		$4+\sqrt{14}$		7
	1	5	23 7		$4+\sqrt{14}$	5	7
	$\sqrt{6}$		57		$7+2\sqrt{14}$		2
	$\sqrt{6}$	5	7		$7+2\sqrt{14}$	5	2
	$2+\sqrt{6}$		3	15	1		2357
	$2+\sqrt{6}$	5	3		1	7	235
	$3+\sqrt{6}$	-	-		$\sqrt{15}$	–	2
	$3+\sqrt{6}$	5	2		$\sqrt{15}$	7	2
7	1		2357		$3+\sqrt{15}$	–	57
	1	3	2 5		$3+\sqrt{15}$	7	5
	$\sqrt{7}$		2		$5+\sqrt{15}$	–	3
	$\sqrt{7}$	3	2 57		$5+\sqrt{15}$	7	3
	$3+\sqrt{7}$		7		$1+\sqrt{15}$	7	35
	$3+\sqrt{7}$	3	57		$15+\sqrt{15}$	7	-
	$7+3\sqrt{7}$		35		$6-\sqrt{15}$	7	2 5
	$7+3\sqrt{7}$	3	5		$5+2\sqrt{15}$	7	23

D	α	l	l_0
21	2		2357
	2	5	23 7
	$2\ \sqrt{21}$	-	2 5
	$2\ \sqrt{21}$	5	2
	$3+\sqrt{21}$	-	2 7
	$3+\sqrt{21}$	5	2 7
	$7+\sqrt{21}$		23
	$7+\sqrt{21}$	5	23
30	1		2357
	1	7	235
	$\sqrt{30}$		
	$\sqrt{30}$	7	
	$5+\sqrt{30}$		3 7
	$5+\sqrt{30}$	7	3
	$6+\sqrt{30}$		5
	$6+\sqrt{30}$	7	5
	$3+\sqrt{30}$ *	7	5
	$10+\sqrt{30}$ *	7	3
	$-4+\sqrt{30}$ *	7	35
	$15-2\ \sqrt{30}$ *	7	2
35	1	-	2357
	$\sqrt{35}$		23
	$5+\sqrt{35}$		7
	$7+\sqrt{35}$		5
42	1		2357
	$\sqrt{42}$		
	$6+\sqrt{42}$		57
	$7+\sqrt{42}$		3
70	1		2357
	1	3	2 57
	$\sqrt{70}$		
	$\sqrt{70}$	3	
	$25+3\ \sqrt{70}$		3 7
	$25+3\ \sqrt{70}$	3	7
	$42+5\ \sqrt{70}$		5
	$42+5\ \sqrt{70}$	3	5
	$7+\sqrt{70}$ *	3	5
	$10+\sqrt{70}$ *	3	7
	[illegible] $+\sqrt{70}$	3	[illegible]
	$35\ \ 4\ \sqrt{70}$ *	3	[illegible]
105	2		2357
	2	3	57
	$2\ \sqrt{105}$		2
	$2\ \sqrt{105}$	2	
	$20+2\ \sqrt{105}$		23 7
	$20+2\ \sqrt{105}$	2	3 7
	$42+4\ \sqrt{105}$		2 5
	$42+4\ \sqrt{105}$	2	5
	$7+\sqrt{105}$ *	2	35
	$15+\sqrt{105}$ *	2	7
	$9+\sqrt{105}$ *	2	57
	$35\ \ 3\ \sqrt{105}$ *	2	3
210	1		2357
	$\sqrt{210}$		

D	a	l	l_0
	$14 + \sqrt{210}$		35
	$15 + \sqrt{210}$		7

D	α	n_e	n_7	[illegible]	[illegible]							
2	1	0	0	0	0	0	0	2 3 5	2 3 5	3	0	3.190×10^{28}
	$\sqrt{2}$	0	0	1	0	0	0	3 5	2 3 5	2	0	3.190×10^{28}
6	1	0	0	0	0	0	0	2 3 7	2 3 7	3	0	2.712×10^{26}
	$\sqrt{6}$	0	0	1	1	0	0	7	2 7	2	0	4.604×10^{22}
	$2+\sqrt{6}$	1	0	1	0	0	0	3	2 3	2	0	2.090×10^{22}
	$3+\sqrt{6}$	1	0	0	1	0	0	2	2 3	3	0	2.090×10^{22}
7	1	0	0	0	0	0	0	2 5 7	2 5 7	2	0	1.065×10^{30}
	$\sqrt{7}$	0	0	0	0	0	1	2 5	2 5	2	0	2.146×10^{28}
	$3+\sqrt{7}$	1	0	1	0	0	0	5 7	2 5 7	1	0	1.065×10^{30}
	$7+3\sqrt{7}$	1	0	1	0	0	1	5	2 5	1	0	2.146×10^{25}
10	1	0	0	0	0	0	0	2 5 7	2 5 7	3	0	3.214×10^{29}
	$\sqrt{10}$	0	0	1	0	1	0	7	2 7	2	0	8.414×10^{24}
	$2+\sqrt{10}$	−1	1	1	0	0	0	5 7	2 5 7	2	1	3.214×10^{29}
	$5+\sqrt{10}$	−1	1	0	0	1	0	2 7	2 7	3	1	8.414×10^{24}
14	1	0	0	0	0	1	0	2 3 7	2 3 7	3	0	4.791×10^{26}
	$\sqrt{14}$	0	0	1	0		1	3	2 3	2	0	4.347×10^{22}
	$4+\sqrt{14}$	1	0	1	0	0	0	7	2 7	2	0	8.143×10^{22}
	$7+2\sqrt{14}$	1	0	[illegible]	1	1	1	2	2	3	0	8.371×10^{18}
15	1	0	0	0	0	0	0	2 3 5	2 3 5	2	0	2.144×10^{28}
	$\sqrt{15}$	0	0		1		0	2	2	2	0	9.427×10^{19}
	$3+\sqrt{15}$	1	0	1			[illegible]	5	2 5	1	0	1.694×10^{24}

	[illegible] + $\sqrt{15}$			[illegible]	[illegible]	[illegible]	0	[illegible]	2 3	1	0	1.635 × 10 [illegible]
	$1 + \sqrt{15}$	[illegible]	[illegible]	[illegible]		0	0	3 5	2 3 5	1	1	2.144 × 10 [illegible]
	[illegible]5 + $\sqrt{15}$	[illegible]	[illegible]		1	[illegible]	0		2	1	1	9.427 × 10 [illegible]
	[illegible] $\sqrt{15}$	[illegible]	[illegible]	0	1	[illegible]	0	2 5	2 5	2	1	1.694×10^{2}
	$5 + 2\sqrt{15}$	1	1	[illegible]	0	1	0	2 3	2 3	2	1	1.035×10^{24}
21	2	0	0	2	0	0	0	2 3 7	2 3 7	1	0	1.898×10^{26}
	2 [illegible] $\sqrt{21}$	0	[illegible]	2	1	0	1	2	2	[illegible]	[illegible]	2.640 × 10 [illegible]
	$3 + \sqrt{21}$	1	0	2	1	0	0	2 7	2 7	[illegible]	0	3.220×10^{22}
	[illegible] + $\sqrt{21}$	[illegible]	0	2	0	0	1	2 3	2 3	1	0	1.435×10^{22}
30	1	0	0	[illegible]	0	0	0	2 3 5	2 3 5	3	0	4.141×10^{28}
	$\sqrt{30}$	0	0	1	1	1	0		2	2	0	2.022×10^{20}
	$5 + \sqrt{30}$	1	0	0	0	1	0	3	2 3	3	0	2.217×10^{21}
	$6 + \sqrt{30}$	1	0	1	1	0	0	5	2 5	2	0	3.276×10^{24}
	$3 + \sqrt{30}$	0	1	0	1	0	0	5	2 5	3	1	3.276×10^{24}
	$10 + \sqrt{30}$	0	1	1	0	1	0	3	2 3	2	1	2.217×10^{21}
	$-4 + \sqrt{30}$	1	1	[illegible]	0	0	0	3 5	2 3 5	2	1	4.141×10^{28}
	$15 - 2\sqrt{30}$	1	1	0	1	1	0	2	2	3	1	2.022×10^{20}
70	1	0	0	0	0	0	0	2 5 7	2 5 7	3	0	3.229×10^{30}
	$\sqrt{70}$	0	0	1	0	1	1		2	2	0	2.115 × 10 [illegible]
	$25 + 3\sqrt{70}$	1	0	0	0	1	0	7	2 7	3	0	8.482×10^{25}
	$42 + 5\sqrt{70}$	1	0	1	0	0	1	5	2 5	2	[illegible]	7.003×10^{25}
	$7 + \sqrt{70}$	0	1	0	0	0	1	5	2 5	3	1	7.003×10^{25}

	$10 + \sqrt{70}$	0	1	1	0	1	0	7	2 7	2	1	$8.482 \times 10^{[illegible]}$
	$8 + \sqrt{70}$	[illegible]	1	1	0	0	0	5 7	2 5 7	2	1	3.229×10^{30}
	$35 - 4\sqrt{70}$	1	1	0	0	1	1	2	2	3	1	2.115×10^{21}
105	2	0	0	2	0	0	0	3 5 7	3 5 7	1	0	4.533×10^{29}
	$2\sqrt{105}$	0	0	2	1	1	1			0	0	$4.295 \times 10^{[illegible]}$
	$20 + 2\sqrt{105}$	1	0	2	0	1	0	3 7	3 7	1	0	1.690×10^{25}
	$42 + 4\sqrt{105}$	1	0	2	1	0	1	5	5	1	0	8.655×10^{20}
	$7 + \sqrt{105}$	0	1	2	0	0	1	3 5	3 5	1	1	1.396×10^{25}
	$15 + \sqrt{105}$	0	1	2	1	1	0	7	7	1	1	1.049×10^{21}
	$-9 + \sqrt{105}$	1	1	2	1	0	0	5 7	5 7	1	1	2.485×10^{25}
	$35 - 3\sqrt{105}$	[illegible]	1	2	0	1	1	3	3	1	1	5.880×10^{20}

Table \

D	A	B	b		m	[illegible] t_1	n_1	a_1	h_2	h_3	h_5	h_7	p = 3 t_1	n_1	a_1	h_2	h_3	h_5	h_7
2	2	−1	1	0	0	2	0	8	3	1	0	0	1	0	12	2	2	1	1
2	2	−1	0	1	0	0							1	6	12	0	2	0	0
3	4	1	1	0	0	3	0	8	4	0	0	1	1	0	9	0	2	1	0
3	4	1	0	1	0	1							0						
3	4	1	1	1	−1	0							1	4	9	0	2	0	0
3	4	1	1	1	−1	0							0						
5	1	−1	2	0	0	4	0	24	5	2	0	1	2	0	36	4	3	0	0
5	1	−1	0	2	0	2							2	18	36	1	3	0	0
6	10	1	1	0	0	3	0	8	4	0	1	2	0	0	3	1	2	0	0
6	10	1	0	1	0	0							0						
6	10	1	2	1	−1	0							2	4	9	0	3	0	0
6	10	1	3	1	−1	0							0						
7	16	1	1	0	0	4	0	4	5	1	0	0	1	0	3	0	2	1	0
7	16	1	0	1	0	3							0						
7	16	1	3	1	−1	0							0						
7	16	1	7	3	−1	0							2	4	9	0	3	1	0
10	6	1	1	0	0	1	0	4	2	1	0	0	1	0	6	1	2	0	0
10	6	−1	0	1	0	0							1	3	6	0	2	0	0
14	30	1	1	0	0	3	0	4	4	1	1	0	1	0	6	3	2	1	0
14	30	1	0	1	0	0							1	3	6	0	2	1	0
14	30	1	4	1	−1	0							0						
14	30	1	7	2	1	1							0						
15	8	1	1	0	0	3	0	4	4	[illegible]	0	0	2	0	9	0	3	0	1
15	8	1	0	1	0	2							0						
15	8	1	3	1	−1	0							0						
15	8	1	5	1	−1	0							2	4	9	0	3	0	0
21	5	1	2	0	0	3	0	6	4	1	1	0	1	0	9	3	2	0	0
21	5	1	0	2	0	1							0						
21	5	1	3	1	1	2							0						
21	5	1	7	1	−1	1							1	4	9	1	2	0	0
30	22	1	1	0	0	1	0	2	2	0	0	0	0	0	3	1	1	0	1
30	22	1	0	1	0	0							0						

D	A	B	b		m	[illegible] t_1	n_1	a_1	h_2	[illegible]	[illegible]	[illegible]	[illegible] t_1	n_1	a_1	h_2	h_3	h_5	h_7
2	2	−1	1	0	0	1	0	15	0	0	2	0	1	0	42	1	0	1	2
2	2	−1	0	1	0	0							1	21	42	0	0	0	2
3	4	1	1	0	0	1	0	15	0	1	2	0	1	0	28	3	0	0	2
3	4	1	0	1	0	0							1	14	28	0	0	0	2
3	4	1	1	1	−1	0							0						
3	4	1	1	1	−1	1	7	15	0	0	2		0						
5	1	−1	2	0	0	1	0	25	0	0	2	0	1	0	56	0	1	0	2
5	1	−1	0	2	0	0							1	28	56	0	0	0	2
6	10	1	1	0	0	1	0	10	2	0	2	0	2	0	28	3	0	1	3
6	10	1	0	1	0	1	5	10	0	0	2		2	14	28	0	0	0	3
6	10	1	2	1	−1	0							0						
6	10	1	3	1	−1	0							0						
7	16	1	1	0	0	0	0	3	0	2	1	0	0	[illegible]	7	0	1	0	1
7	16	1	0	1	0	0							0						
7	16	1	3	1	−1	0							0	3	7	0	0	0	1
7	16	1	7	3	−1	1	7	15	0	2	2	0	0						
10	6	1	1	0	0	0	0	5	0	0	1	0	0	0	8	3	1	0	1
10	6	−1	0	1	0	0							0	4	8	0	0	0	1
14	30	1	1	0	0	1	0	10	3	1	2	0	0	0	7	2	0	0	1
14	30	1	0	1	0	1	5	10	0	1	2	0	0						
14	30	1	4	1	−1	0							0	3	7	0	0	0	1
14	30	1	7	2	1	0							0						
15	8	1	1	0	0	0	0	5	0	0	1	0	1	0	21	0	2	0	2
15	8	1	0	1	0	0							0						
15	8	1	3	1	−1	0	2	5	0	0	1	0	1	10	21	0	0	0	2
15	8	1	5	1	−1	0							0						
21	5	1	2	0	0	1	0	10	0	0	2	0	0	0		0	0	0	1
21	5	1	0	2	0	1	5	10	0	0	2	0	0						
21	5	1	3	1	1	0							0		7	0	0	0	1
21	5	1	7	1	−1	0							0						
30	22	1	1	0	0	0	0	5	[illegible]	[illegible]	[illegible]	[illegible]	0		3	[illegible]	[illegible]	[illegible]	[illegible]
30	22	1	0	1	0	0							0						

D	A	B	a	b	n_0	p = 2 t_1	n_1	a_1	h_2	h_3	h_5	h_7	p = 3 t_1	n_1	a_1	h_2	h_3	h_5	h_7	p = 5 t_1	n_1	a_1	h_2	h_3	h_5	h_7	p = 7 t_1	n_1	a_1	h_2	h_3	h_5	h_7
30	22	1	5	1	−1	0							1	4	9	0	2	0	1	0							1	10	21	0	1	0	2
30	22	1	6	1	−1	0							0							0	2	5	0	0	1	0	0						
35	12	1	1	0	0	2	0	4	3	1	0	0	1	0	6	2	2	0	0	0	0	5	0	0	1	0	0	0	7	0	0	0	1
35	12	1	0	1	0	1							1	3	6	1	2	0	0	0							0						
35	12	1	5	1	−1	0							0							0							0	3	7	0	0	0	1
35	12	1	7	1	−1	0							0							0	2	5	0	0	1	0	0						
42	26	1	1	0	0	1	0	2	2	0	0	0	3	0	9	1	4	2	0	2	0	15	1	3	3	0	0	0	7	1	0	0	1
42	26	1	0	1	0	0							0							0							0						
42	26	1	6	1	−1	0							0							2	7	15	0	0	3	0	0	3	7	0	0	0	1
42	26	1	7	1	−1	0							3	4	9	0	4	0	0	0							0						
70	502	1	1	0	0	1	0	2	2	1	1	0	1	0	3	1	2	1	0	1	0	5	1	1	2	0	0	0	7	1	1	1	1
70	502	1	0	1	0	0							0							0							0						
70	502	1	25	3	−1	0							1	1	3	0	2	0	0	0							0	3	7	0	1	0	1
70	502	1	42	5	−1	0							0							1	2	5	0	0	2	0	0						
105	82	1	2	0	0	3	0	2	4	0	0	0	0	0	3	3	4	0	0	0	0	5	3	0	1	0	0	0	7	3	0	0	1
105	82	1	0	2	0	1							0							0							0						
105	82	1	20	2	−1	1							4	4	9	1	5	0	0	0							0	3	7	1	0	0	1
105	82	1	42	4	−1	2							0							0	2	5	2	0	1	0	0						
210	58	1	1	0	0	1	0	2	2	0	0	0	0	0	3	1	1	0	0	0	0	5	1	0	1	0	0	0	7	1	0	0	1
210	58	1	0	1	0	0							0							0							0						
210	58	1	14	1	−1	0							0	1	3	0	1	0	0	0	2	5	0	0	1	0	0						
210	58	1	15	1	−1	0							0							0							0	3	7	0	0	0	1

Table VI

D	p_i	v_i	λ_i		
2	2 3 5	3 0 0	1.5	0	0
6	2 3 7	3 1 0	1.5	0.5	0
7	2 5 7	2 0 1	1	0	0.5
10	2 5 7	3 1 0	1.5	0.5	0
14	2 3 7	3 0 1	1.5	0	0.5
15	2 3 5	2 1 1	1	.05	0.5
21	2 3 7	2 1 1	0	0.5	0.5
30	2 3 5	3 1 1	1.5	0.5	0.5
70	2 5 7	3 1 1	1.5	0.5	0.5
105	3 5 7	1 1 1	0.5	0.5	0.5

第八章 Thue 方程

8.1 导言

设 $F(X,Y)\in Z[X,Y]$是带整系数，次数至少是 3 的既约二元型．m 是非零整数．丢番图方程

$$F(X,Y)=m \quad X,Y\in Z$$

称为 Thue 方程．它在丢番图方程理论中起主要作用．1909 年，Thue[115]证明它仅有有限多个解．他的证明是非实效的．此类方程解的可有效计算的上界是由 Baker[8]首先给出的(参见 Shorey 和 Tijdeman[10]第 5 章关于 Thue 方程结果的综述)．通过运用引理 2·4，我们得到 Thue 方程解的更好的上界，目前这方面的最好结果是由 Bugeaud 和 Gyory[29]得到的．然后，我们说明为什么在第 3 章产生的方法能实际用于找出 Thue 方程的全部解．我们的方法主要研究任意 Thue 方程，而实际上是次数不太大的 Thue 方方假如关于型 F 的某代数数据是有效的．看 Tzanakis[123]中的简短导言．

我们这里使用的不同方法已被 Ellison, Ellison, Pesek, Stahl 和 Stall[38], Steiner[110], Pethö 和 Schulenberg[92], Blass, Glass, Meronk 和 Steiner[17],[18]实际用于解 Thue 方程．所有这些情形，都取 $m=1$，而 de Weger[137],[138]运用本章叙述的方法解决了满足 $m>1$ 的例子．在确定斐波那契序列中所有三次幂时，Pethö[90]用 Gelfond - Baker 方法解

Thue 方程，但他用完全不同的方法求出上界之下的全部解．而多数 Thue 方程必须用不同的(通常是特定的)方法求解．

8·2 从 Thue 方程到对数线性型

本节中，我们表明，一般的 Thue 方程怎样导出不等式，此不等式含有带有理整系数(未知)的代数数对数线性型．设

$$F(X, Y) = \sum_{i=0}^{n} f_i \cdot X^{n-i} \cdot Y^i \in Z[X, Y]$$

是次数 $n \geqslant 3$ 的二元型，又设 m 是一个非零整数．考虑 Thue 方程

$$F(X, Y) = m \qquad (8 \cdot 1)$$

其中未知数 $X, Y \in Z$．若 F 在 Q 上是可约的，则(8·1)可简化成具有既约二元型的形如(8·1)的有限多个方程的方程组．对次数 1 或 2 的这样的方程，熟知怎样确定其解．因此从现在起，我们可假定 F 在 Q 上是既约的且次数 $\geqslant 3$．设 $g(X) = F(X, 1)$．若 $g(X) = 0$ 没有实根，则对(8·1)的解 (X, Y)，可平常地找到关于 $\max(|X|, |Y|)$ 的小的上界．因此，贯穿本章，我们假定代数方程 $g(X) = 0$ 至少有一个实根．我们给它的根编号如下：$\xi^{(1)}, \cdots, \xi^{(s)}$ (满足 $s \geqslant 1$) 是实根而 $\xi^{(s+1)} = \overline{\xi^{(s+t+1)}}, \cdots, \xi^{(s+t)} = \overline{\xi^{(s+2t)}}$ 是非实根，因此我们有 $t(\geqslant 0)$ 对复共轭根．且 $s + 2 \cdot t = n$．

考虑域 $K = Q(\xi)$，其中 $g(\xi) = 0$．我们规定三个正实数 $Y_1 < Y_2 < Y_3$，将(8·1)的可能的解 (X, Y) 的集分为四种情形：

→"很小"解，满足$|Y|\leqslant Y_1$. 用列举所有可能的方法求出这些解.

→"小"解，满足$Y_1<|Y|\leqslant Y_2$. 通过实根$\xi^{(i)}$的连分数展式的值的计算来求这些解.

→"大"解，满足$Y_2<|Y|\leqslant Y_3$. 通过计算的丢番图逼近方法来证明这样的解不存在.

→"很大"解，满足$|Y|>Y_3$. 用对数线性型理论来证明不存在这样的解.

Y_3的值由对数线性型的 Gelfond - Baker 理论导出. Y_2的值，用我们证明没有"大"解存在所作的限制来导出. Y_1的值由下面引理 8·1 导出，这个引理表明，若$|Y|$足够大，则X/Y"极端接近"一个实根$\xi^{(i)}$. 在一个典型例子中，Y_3可大如$10^{10^{50}}$，Y_2大如10^{10}，Y_1小如 10.

引理 8·1　设$X, Y\in Z$满足(8·1)，令$\beta = X-\xi\cdot Y$,

$$Y_0=\begin{cases}\left[\left[\dfrac{2^{n-1}\cdot|m|}{\min\limits_{1\leqslant i\leqslant t}|g'(\xi^{(s+i)})|\cdot\min\limits_{1\leqslant i\leqslant t}|\mathrm{Im}\xi^{(s+i)}|}\right]^{1/n}\right] & 若\ t\geqslant 1\\ 1 & 若\ t=0\end{cases},$$

$$C_1=\frac{2^{n-1}\cdot|m|}{\min\limits_{1\leqslant i\leqslant s}|g'(\xi^{(i)})|},\ C_2=\frac{1}{2}\cdot\min_{1\leqslant i<j\leqslant n}|\xi^{(i)}-\xi^{(j)}|,$$

$$Y_1=\max[Y_0\cdot[[4\cdot C_1]^{1/(n-2)}]].$$

(i)若$|Y|>Y_0$，则存在一个$i_0\in\{1,\cdots,s\}$使得

$$|\beta^{(i_0)}|\leqslant C_1\cdot|Y|^{-(n-1)},$$

$$|\beta^{(i)}|\geqslant C_2\cdot|Y|,\ i\in\{1,\cdots,n\};i\neq i_0.$$

(ii)若$|Y|>Y_1$，则 X/Y 从 $\xi^{(i_0)}$的连分数展式收敛.

证明 设 $i_0\in\{1,\cdots,n\}$使得$|\beta^{(i_0)}|=\min_{1\leqslant i\leqslant n}|\beta^{(i)}|$. 由(8·1)，我们有

$$|f_0|\cdot\prod_{i=1}^{n}|\beta^{(i)}|=|m|.$$

由$|\beta^{(i_0)}|$的最小值，对所有 i 有

$$|Y|\cdot|\xi^{(i)}-\xi^{(i_0)}|=|\beta^{(i)}-\beta^{(i_0)}|\leqslant|\beta^{(i)}|+|\beta^{(i_0)}|$$
$$\leqslant 2\cdot|\beta^{(i)}|.$$

因此$|\beta^{(i)}|\geqslant C_2\cdot|Y|$. 进而，

$$|\beta^{(i_0)}|=\frac{|m|}{|f_0|}\cdot\prod_{i\neq i_0}|\beta^{(i)}|^{-1}\leqslant\frac{|m|}{|f_0|}\cdot\prod_{i\neq i_0}\left[\frac{1}{2}\cdot|Y|\cdot|\xi^{(i)}-\xi^{(i_0)}|\right]^{-1}$$

$$=\frac{2^{n-1}\cdot|m|}{|f_0\cdot\prod_{i\neq i_0}(\xi^{(i)}-\xi^{(i_0)}|\cdot|Y|^{n-1}}=\frac{2^{n-1}\cdot|m|}{|g'(\xi^{(i_0)})|\cdot|Y|^{n-1}}.$$

现在，若 $i_0>s$(因此 $t\geqslant1$)，则由 Y_0 的定义，

$$\left|\frac{X}{Y}-\xi^{(i_0)}\right|=\frac{|\beta^{(i_0)}|}{|Y|}\leqslant\frac{2^{n-1}\cdot|m|}{|g'(\xi^{(i_0)})|}\cdot|Y|^{-n}$$
$$\leqslant\left[\frac{Y_0}{|Y|}\right]^n\cdot\min_{s+1\leqslant i\leqslant s+t}|\mathrm{Im}\xi^{(i)}|,$$

由于$|Y|>Y_0$，故这不可能. 因此 $i_0\leqslant s$，从而(i)立即导出. 再者，若$|Y|>Y_1$，则

$$\left|\frac{X}{Y}-\xi^{(i_0)}\right|=|\beta^{(i_0)}|\cdot|Y|^{-1}\leqslant C_1\cdot|Y|^{-n}\leqslant\frac{1}{4}\cdot Y_1^{n-2}\cdot|Y$$

$|\quad|^n \leqslant \frac{1}{2}|Y|^{-2}$,

因此，$\left|\frac{X}{Y}-\xi^{(i_0)}\right|<\frac{1}{2}\cdot|Y|^{-2}$，因 $\xi^{(i_0)}$ 是无理数. 现在，由熟知的连分数的结果(见(3·6))即导出(ii).

现在，如引理 8·1，设 $|Y|>Y_1$，$i\in\{1,\cdots,s\}$，选择 $j,k\in\{1,\cdots,n\}$ 使得 i_0,j,k 是两两不同的；且或者 $j,k\in\{1,\cdots,s\}$ 或者 $j+t=k$(因此 $\xi^{(k)}=\overline{\xi^{(j)}}$，但进而，$j,k$ 的选取是无约束的. 由于对 $i=i_0,j,k$ 有 $\beta^{(i)}=X-Y\cdot\xi^{(i)}$，消去 X 和 Y 我们得

$$\beta^{(i_0)}\cdot[\xi^{(j)}-\xi^{(k)}]+\beta^{(j)}\cdot[\xi^{(k)}-\xi^{(i_0)}]+\beta^{(k)}\cdot[\xi^{(i_0)}-\xi^{(j)}]=0,$$

或者，等价地，

$$\frac{\xi^{(i_0)}-\xi^{(j)}}{\xi^{(i_0)}-\xi^{(k)}}\cdot\frac{\beta^{(k)}}{\beta^{(j)}}-1=-\frac{\xi^{(k)}-\xi^{(j)}}{\xi^{(k)}-\xi^{(i_0)}}\cdot\frac{\beta^{(i_0)}}{\beta^{(j)}} \qquad (8\cdot2)$$

由引理 8·1，上式右边"极端小". 设，若 $j,k\in\{1,\cdots,s\}$（让我们称其为"实情形"），则

$$\Lambda=\log\left|\frac{\xi^{(i_0)}-\xi^{(j)}}{\xi^{(i_0)}-\xi^{(k)}}\cdot\frac{\beta^{(k)}}{\beta^{(j)}}\right|.$$

而当 $j,k\in\{s+1,\cdots,s+2\cdot t\}$（让我们称其为"复情形"）时，

$$\Lambda=\frac{1}{i}\log\left|\frac{\xi^{(i_0)}-\xi^{(j)}}{\xi^{(i_0)}-\xi^{(k)}}\cdot\frac{\beta^{(k)}}{\beta^{(j)}}\right|.$$

这儿，一般的，对 $z\in C$，$\log z$ 表示 z 的对数的主值(因此 $-\pi<\operatorname{Im}\log(z)\leqslant\pi$). 由 $\xi^{(k)}=\overline{\xi^{(j)}}$，我们有 $\Lambda\in R$ 及 $|\Lambda|\leqslant\pi$.

下面引理显示 $|\Lambda|$ 有多小.

引理 8·2　设

$$C_3 = \max_{i_1 \neq i_2 \neq i_3 \neq i_1} \left| \frac{\xi^{(i_1)} - \xi^{(i_2)}}{\xi^{(i_1)} - \xi^{(i_3)}} \right|,$$

$$Y_2^* = \max[Y_1, [(2 \cdot C_1 \cdot C_3 / C_2)^{1/n}]].$$

若 $|Y| > Y_2^*$ 则

$$|\Lambda| < \frac{1.39 \cdot C_1 \cdot C_3}{C_2} \cdot |Y|^{-n}.$$

证明　首先考虑实情形. 由 $|Y| > Y_2^*$ 及引理 8·1 导出, (8·2)的右边绝对值小于 $\frac{1}{2}$, 从而

$$\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\beta^{(k)}}{\beta^{(j)}} > 0.$$

由此导出(8·2)的左边等于 $e^{\Lambda} - 1$, 由引理 8·1 的观察及 C_3 的定义, 现在(8·2)蕴涵

$$|e^{\Lambda} - 1| < C_3 \cdot \frac{C_1 \cdot |Y|^{-(n-1)}}{C_2 \cdot |Y|} = \frac{C_1 \cdot C_3}{C_2} \cdot |Y|^{-n}.$$

另一方面, $|e^{\Lambda} - 1| < \frac{1}{2}$ 蕴涵(参见引理 2·2)

$$|\Lambda| \leqslant 2 \cdot \log 2 \cdot |e^{\Lambda} - 1| \leqslant 1.39 \cdot |e^{\Lambda} - 1|,$$

这就证明了在实情形我们的断言.

在复情形, (8·2)的左边等于 $e^{i\Lambda} - 1$, 如同实情形, 我们导出

$$|e^{i\Lambda} - 1| < \frac{C_1 \cdot C_3}{C_2} \cdot |Y|^{-n} < \frac{1}{2}.$$

因为 $|e^{i\Lambda} - 1| = 2 \cdot |\sin \Lambda/2|$, 导出了 $|\sin \Lambda/2| < \frac{1}{4}$, 因此由

引理 2·3

$$|\Lambda| = 2\cdot\frac{1/4}{\sin 1/4}\cdot|\sin\Lambda/2| = \frac{1/4}{\sin 1/4}\cdot|e^{i\Lambda}-1| \leqslant 1.02\cdot$$
$e^{i\Lambda-1}|$。

这就证明了在复情形引理成立.

在域 K 的整数环(也在任意其他 K 的阶 R)中存在基本单位组 $\varepsilon_1, \cdots, \varepsilon_r$, 其中 $r = s + t - 1$(Dirichlet 的基本定理). 注意到由于 F 是既约的且我们已假定 $s>0$, 故属于 K 的仅有单位根是 ± 1. 这里我们不准备讨论求这单位组的问题(有效的方法看例如 Berwick[13], Billevič[15], [16], Pohst 和 Zassenhaus[97], Buchmann[27], [28]. 我们简单地假定基本单位组是已知的, 另一方面, 仅存在有限多个 K 中的非共轭 $\mu_1, \cdots, \mu_\nu$ 使得 $f_0\cdot N(\mu_i) = m$ 对 $i = 1, \cdots, \nu$ 成立(我们用 $N(\cdot)$ 来表示扩张 K/Q 的范数). 我们也假定这样的 μ_i 的全集是已知的. 设 M 是所有 $\zeta\cdot\mu_i$ 的集合, 其中 ζ 是 K 中的单位根. (在重要情形 $|f_0| = |m| = 1$, 显然 $M = \{-1, 1\}$). 则对(8·1)的任意整数解(X, Y), 存在某个 $\mu\in M$ 及 $a_1, \cdots, a_r\in Z$, 使得

$$\beta = \mu\cdot\varepsilon_1^{a_1}\cdot\cdots\cdot\varepsilon_r^{a_r}.$$

因此, 解(8·1)的初始问题是简化为求所有的整 r - tuples$(a_1, \cdots, a_r)$使得 $\mu\cdot\varepsilon_1^{a_1}\cdot\cdots\cdot\varepsilon_r^{a_r}$ 对某 $\mu\in M$ 是特殊形式 $X - Y\cdot\xi$, 满足 $X, Y\in Z$. 正如我们已看到的, X 和 Y 可以消去, 因此得到(8·2). 故问题简化为解有限多个方程, 形如

$$\frac{\xi^{(i_0)}-\xi^{(j)}}{\xi^{(i_0)}-\xi^{(k)}}\cdot\frac{\mu^{(k)}}{\mu^{(j)}}\cdot\prod_{i=1}^{r}\left[\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right]^{a_i}-1$$

$$=-\frac{\xi^{(k)}-\xi^{(j)}}{\xi^{(k)}-\xi^{(i_0)}}\cdot\frac{\mu^{(i_0)}}{\mu^{(j)}}\cdot\prod_{i=1}^{r}\left[\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}\right]^{a_i}.$$

(所谓的"单位方程").在实情形有

$$\Lambda=\log\left|\frac{\xi^{(i_0)}-\xi^{(j)}}{\xi^{(i_0)}-\xi^{(k)}}\cdot\frac{\mu^{(k)}}{\mu^{(j)}}\right|+\sum_{i=1}^{r}a_i\cdot\log\left|\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right|, \tag{8·3}$$

而在复情形有

$$\Lambda=\mathrm{Arg}\left[\frac{\xi^{(i_0)}-\xi^{(j)}}{\xi^{(i_0)}-\xi^{(k)}}\cdot\frac{\mu^{(k)}}{\mu^{(j)}}\right]+\sum_{i=1}^{r}a_i\cdot\mathrm{Arg}\left[\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right]+a_j\cdot 2\pi, \tag{8·4}$$

其中 $a_0\in Z$, $-\pi<\mathrm{Arg}(z)\leqslant\pi$, $z\in C$. 注意实情形的 Λ 及复情形 $|\Lambda|$(主部)都是代数数对线线性型,其中系数 a_i 是整数. Gelfond-Baker 理论根据 $\max|a_i|$ 提供关于 $|\Lambda|$ 的一个显示上界. 由此并结合引理 8·2 我们可找到关于 $\max|a_i|$ 的一个显示上界. 这就是我们下节所要做的.

8·3 上界

设 $A=\max\limits_{1\leqslant i\leqslant r}|a_i|$. 首先我们根据 $|Y|$ 找出关于 A 的一个上界.

引理 8·3　设 $I=\{h_1,\cdots,h_r\}\subset\{1,\cdots,n\}$. 令

$$U_I=[\log|\varepsilon_\iota^{h_i}|]_{1\leqslant i\leqslant r,1\leqslant\iota\leqslant r},$$

(其中 i,ι 分别表示矩阵的行，列)，

$$U_I^{-1}=(u_{i\iota}),\quad N[U_I^{-1}]=\max_{1\leqslant\iota\leqslant n-1}\sum^{r}|u_{i\iota}|.$$

又设

$$\mu_-=\min_{\substack{1\leqslant i\leqslant n\\ \mu\in M}}|\mu^{(i)}|,\quad \mu_+=\max_{\substack{1\leqslant i\leqslant n\\ \mu\in M}}|\mu^{(i)}|,$$

$$C_4=\frac{\frac{1}{2}+\max\limits_{1\leqslant i_1<i_2\leqslant n}|\xi^{(i_1)}-\xi^{(i_2)}|}{\mu_-},$$

$$C_5=\min[(n-1)\cdot\min_I N[U_I^{-1}],\max_I[U_I^{-1}]]$$

则对

$$|Y|>\max[Y_1,2\cdot|m|^{1/n},\mu_+/C_2],$$

我们有

$$A<C_5\cdot\log[C_4\cdot|Y|].$$

证　由 $\beta=\mu\cdot\varepsilon_1^{a_1},\cdots,\varepsilon_r^{a_r}$，我们有

$$\begin{bmatrix}\log|\beta^{(h_1)}/\mu^{(h_1)}|\\ \cdots\\ \log|\beta^{(h_r)}/\mu^{(h_r)}|\end{bmatrix}=U_I\cdot\begin{bmatrix}a_1\\ \cdots\\ a_r\end{bmatrix}\tag{8·5}$$

另一方面，对每个 $h\in\{1,\cdots,n\}$，利用引理 8·1 证明的末尾，

$$|\beta^{(h)}| = |X - Y\cdot\xi^{(h)}| \leqslant |X - Y\cdot\xi^{(i_0)}| + |Y|\cdot|\xi^{(i_0)} - \xi^{(h)}|$$

$$\leqslant \frac{1}{2\cdot|Y|} + |Y|\cdot|\xi^{(i_0)} - \xi^{(h)}|$$

$$\leqslant [\frac{1}{2} + \max_{1\leqslant i_1 < i_2 \leqslant n} |\xi^{(i_1)} - \xi^{(i_2)}|]\cdot|Y|,$$

因此

$$\left|\frac{\beta^{(h)}}{\mu^{(h)}}\right| < C_4|Y|, \quad h = 1, \cdots, n.$$

注意 $C_4\cdot|Y| > 1$. 实际上，由

$$\prod_{i=1}^{n} |\mu^{(i)}| = \frac{|m|}{|f_0|} \leqslant |m|$$

导出 $\min_{1\leqslant i\leqslant n} |\mu^{(i)}| \leqslant |m|^{1/n}$，因此 $\mu_- \leqslant |m|^{1/n}$. 因此

$$C_4\cdot|Y| \geqslant [\frac{1}{2} + \max_{1\leqslant i_1 < i_2 \leqslant n} |\xi^{(i_1)} - \xi^{(i_2)}|]\cdot|Y|\cdot|m|^{-1/n}$$

$$> \frac{|Y|}{2\cdot|m|^{1/n}} > 1.$$

则

$$\log\left|\frac{\beta^{(h)}}{\mu^{(h)}}\right| < \log[C_4\cdot|Y|], \quad h = 1, \cdots, n,$$

$$\log[C_4\cdot|Y|] > 0. \tag{8·6}$$

其次我们证

$$\left|\log\left|\frac{\beta^{(i)}}{\mu^{(i)}}\right|\right|<(n-1)\cdot\log[C_4\cdot|Y|],i=1,\cdots,n. \qquad (8\cdot 7)$$

事实上，考察(8·6)，若$|\beta^{(i)}/\mu^{(i)}|\geqslant 1$，则更强的不等式成立．现假定$|\beta^{(i)}/\mu^{(i)}|<1$，由

$$\prod_{h=1}^{n}\left|\frac{\beta^{(h)}}{\mu^{(h)}}\right|=1$$

导出

$$\left|\log\left|\frac{\beta^{(i)}}{\mu^{(i)}}\right|\right|=-\log\left|\frac{\beta^{(i)}}{\mu^{(i)}}\right|=\sum_{\substack{h=1\\h\neq i}}^{n}\log\left|\frac{\beta^{(h)}}{\mu^{(h)}}\right|<(n-1)\cdot\log$$

$[C_4\cdot|Y|]$，

考虑(8·6)，不等式

$$A<(n-1)\cdot\min N[U_I^{-1}]\cdot\log[C_4\cdot|Y|]$$

由(8·5)，(8·7)导出$N[U_I^{-1}]$的定义以及到目前我们对I不设任何限制的事实，便可选择$N[U_I^{-1}]$为最小的．剩下的是证

$$A<\max_I N[U_I^{-1}]\cdot\log[C_4\cdot|Y|].$$

选择I的使得$i_0\in I$．则由引理8·1，对每个$h\in I$，$|\beta^{(h)}/\mu^{(h)}|>C_2\cdot|Y|/\mu_+>1$，考察(8·6)，现在

$$\left|\log\left|\frac{\beta^{(h)}}{\mu^{(h)}}\right|\right|<\log[C_4\cdot|Y|],$$

这蕴涵我们的结论．

引理 8·2 和 8·3 直接导出.

引理 8·4　设

$$C_6 = \frac{1.39 \cdot C_1 \cdot C_3 \cdot C_4^n}{C_2},$$

$$Y'_2 = \max[Y_2', 2 \cdot |m|^{1/n}, \mu_+ / C_2].$$

若 $|Y| > Y'_2$ 则

$$|\Lambda| < C_6 \cdot \exp[\frac{-n}{C_5} \cdot A].$$

下面, 我们应用引理 2·4, 导出在实情形(假定 $\Lambda \neq 0$)

$$|\Lambda| > \exp[-C_7 \cdot (\log A + C_8)]. \tag{8·8}$$

而在复情形, 当 A 用 $A' = \max\limits_{0 \leq i \leq r} |a_i|$ 代替时, 上式也成立. C_7 和 C_8 的精确值已在 2·3 节给出. 必须注意的是在复情形, 现在引起了 a_0 的出现, 而不是在引理 8·3 和 8·4 呈现的. 为了得到 A 的上界, 我们必须根据 A 来找到 A' 的一个上界. 事实上, 由

$$\mathrm{Arg}(z_1 \cdot z_2) = \mathrm{Arg}(z_1) + \mathrm{Arg}(z_2) + K \cdot 2\pi,$$
$$K \in \{-1, 0, 1\},$$

我们从(8·4)及引理 8·2 的证明发现, 若 $A \geq 2$, 则

$$|a_0| < \frac{1}{2} + \frac{1}{2} \cdot r \cdot A + |\Lambda|/2\pi < 1 + r \cdot A$$
$$\leq r \cdot A$$

因此若用

$$C'_8 = C_8, \text{实情形}$$

$$C'_8 = C_8 + \log r, \text{复情形}$$

代替 C_8，我们可应用(8·8)到具有相同的 Λ 的两种情形. 现在，我们可给出关于 A 的上.

引理 8·5　设

$$C_9 = \frac{2 \cdot C_5}{n}[\log C_6 + C_7 \cdot C_8' + C_7 \cdot \log \frac{C_5 \cdot C_7}{n}].$$

若 $|Y| > Y'_2$，则 $A < C_9$.

证明　证明引理 8·2 时我们已看出，在实情形，$|e^\Lambda - 1| < \frac{1}{2}$；在复情形，$|e^{i\Lambda} - 1| < \frac{1}{2}$. 注意 $\beta^{(i_0)} \neq 0$. 因此(8·2)蕴涵 $\Lambda \neq 0$. 从而由引理 8·4 和(8·8)导出

$$A < \frac{C_5}{n} \cdot [\log C_6 + C_7 \cdot C_8' + C_7 \cdot \log A].$$

由引理 2·1 导出结果.

注释　由 A 的这个上界可导出 $|Y|$ 的上界，从而导出 Y_3 的值(见 8·2 节)，我们不具体求出. 注意 Y_2'(见引理 8·4)等于 Y_2 不是必要的(见 8·2 节).

8·4　简化上界

现在我们剩下下面类型的问题. 设给出实数 $\delta, \mu_1, \cdots, \mu_q$

($q\geqslant 2$, $q=1$ 的情形是平凡的). 记

$$\Lambda = \delta + a_1\mu_1 + \cdots + a_q\mu_q,$$

其中 a_i 的归属是 Z, 并令 $A = \max\limits_{1\leqslant i\leqslant q}|a_i|$. 若 K_1, K_2, K_3 是给出的正数, 则找到所有 q - tuples$(a_1, \cdots, a_q)\in Z^q$ 满足

$$|\Lambda| < K_1\cdot\exp[-K_2\cdot A], \quad A < K_3. \tag{8·9}$$

对我们的情形, 由(8·3)和(8·4)导出如何定义 q, δ 及 μ_i, 从引理 8·4 和 8·5 如何定义 K_1, K_2, K_3. 一般 K_1, K_2 是"小"常数, 而 K_3"很大". 令

$$\Lambda_0 = a_1\mu_1 + \cdots + a_q\mu_q.$$

因此 $\Lambda = \delta + \Lambda_0$. 我们应用第三章处理问题(8·9)的方法.

下面我们区别三种情形. 在前两种情形我们假定 μ_i 是 Q - 无关的.

(i) 设 $\delta = 0$, 这样 $\Lambda = \Lambda_0$. 则其线性型是齐次的, 我们应用 3·7 节的方法.

(ii) 设 $\delta\neq 0$. 则其线性型是非齐次的, 我们应用 3·8 节的方法.

(iii) 现假定 μ_i 是 Q - 相关的. 设 Γ 是线性型 Λ 的逼近格, 如 3·7 节所定义的. 则我们期待 $|\underline{x}|$ $(\underline{x}\in\Gamma, \underline{x}\neq 0)$ 的下界一般是"非常小", 因为向量作为坐标有相关关系系数将引起格中很短的向量. 因此, 简化过程作为前二种情况的应用将不进行. 在这种情形我们进行如下. 设 M 是 $\{\mu_1, \cdots, \mu_q\}$ 的 Q - 无关数组成的极大子集. 对于下标的适当选择我们可假定 $M = \{\mu_1, \cdots, \mu_p\}$, $p<q$. 则对 $1\leqslant i\leqslant p<j\leqslant q$, 我们可找到整数 d

>0 及 $d_{i,j}$使得

$$d \cdot \mu_j = \sum_{i=1}^{p} d_{ij} \cdot \mu_i, \quad j = P+1, \cdots, q.$$

(这些数 d, d_{ij}可以按照在简化基中极端短向量的坐标找到)

另一方面,(8·9)等价于

$$|\Lambda'| < K_1' \cdot \exp[-K_2 \cdot A], \quad A < K_3, \qquad (8\cdot10)$$

其中 $\Lambda' = d \cdot \Lambda$, $K_1' = d \cdot K_1$. 现在,满足 $\delta' = d \cdot \delta$ 以及

$$a_i' = d \cdot a_i + \sum_{j=p+1}^{q} d_{ij} \cdot a_j$$

我们得

$$\Lambda' = \delta' + \sum_{i=1}^{p} a_i' \cdot \mu_i.$$

设 $D = \max\{|d|, |d_{ij}| : 1 \leqslant i \leqslant p < j \leqslant q\}$. 则

$$|a_i'| \leqslant (q-p+1) \cdot D \cdot A, \quad i = 1, \cdots, p.$$

因此,令 $A' = \max_{1 \leqslant i \leqslant p} |a_i'|$, 则 $A' \leqslant (q-p+1) \cdot D \cdot A$, (8·10)蕴含

$$|\Lambda'| < K_1' \cdot \exp[-K_2' \cdot A'], \quad A' < K_3', \qquad (8\cdot11)$$

其中,

$$\Lambda' = \delta' + a_1' \cdot \mu_1' + \cdots + a_p' \cdot \mu_p', \quad K_1' = d \cdot K_1,$$

$$K'_2 = K_2/(q-1+p)\cdot D,\ K_3' = (q-p+1)\cdot K_3.$$

现在，为解(8·11)我们应用(i)或(ii)中叙述的简化过程．或者与$\delta'=0$或者与$\delta'\neq 0$相关，并可多次使用，若必要的话，直至找到A'的很小的上界．在找到(8·11)的所有解$(a_1', \cdots, a_p')$之后，我们有关于$|\Lambda'|$的下界$L>0$．期待L不是"极端小"是合情合理的，因为整数$a_1', \cdots, a_p'$的绝对值"小"不能使$|\Lambda'|$"极端小"．现在结合$|\Lambda'|\geqslant L$以及(8·10)的第一个不等式，得到

$$A < \frac{1}{K_2}\cdot \log[\frac{K_1}{L}].$$

因为L不是"非常小"，作为启发地表明，A的上述上界是"小的"．

现在回到一般情形，我们指出，若A的简化上界(在上面叙述的简化步骤之后找到)不是小得足以在适当的时间内容许列举剩下的可能，那么，应用Fincke和Pohst方法是必要的，或者说至少是可取的，参见3·6节．然而，当解Thue方程，而不仅是对数线性型不等式时，最好是避免这种方法，而采用根$\xi^{(i)}$的连分数．实际上，我们可以搜寻(8·1)满足$Y_1<|Y|\leqslant C$的解(X, Y)如下，提及引理8·1，这儿例如$C=Y_2$，我们可想象这里C是较Y_1大的一个"大"常数，但不是"非常大"(见8·2节中Y_1, Y_2的导入)．

设$\bar{\xi}$是$\xi^{(i_0)}$的有理逼近，使得

$$|\bar{\xi} - \xi^{(i_0)}| < \frac{1}{6\cdot C^2} \qquad (8\cdot 12)$$

因为$|Y|>Y_1$，由$\xi^{(i_0)}$的连分数表示式，X/Y必是收敛的，比如p_k/q_k．用$a_0, a_1, a_2, \cdots$表示此表示式的部分商．首先我们要

求 $a_{k+1}\geqslant 3$. 实际上, 由(3·5)

$$\frac{1}{(a_{k+1}+2)\cdot|Y|^2}\leqslant\frac{1}{(a_{k+1}+2)\cdot q_k^2}$$

$$<\left|\xi^{(i_0)}-\frac{p_k}{q_k}\right|=\left|\xi^{(i_0)}-\frac{X}{Y}\right|\leqslant\frac{C_1}{|Y|^n}.$$ 若 $a_{k+1}=1$ 或 2, 则我们必有 $|Y|^{n-2}<4\cdot C_1$. 因此, 这是荒谬的, 因为 $|Y|>Y_1>(4\cdot C_1)^{1/(n-2)}$. 因此 $a_{k+1}\geqslant 3$, 又由(3·5)我们得

$$\left|\xi^{(i_0)}-\frac{p_k}{q_k}\right|<\frac{1}{a_{k+1}\cdot q_k^2}\leqslant\frac{1}{3\cdot q_k^2}.$$

因此

$$\left|\bar{\xi}-\frac{p_k}{q_k}\right|\leqslant|\bar{\xi}-\xi^{(i_0)}|+\left|\xi^{(i_0)}-\frac{p_k}{q_k}\right|$$

$$<\frac{1}{6\cdot C^2}+\frac{1}{3\cdot q_k^2}\leqslant\frac{1}{2\cdot q_k^2}.$$

而这意味着 p_k/q_k 事实上也是由 $\bar{\xi}$ 的连分数表示式的收敛. 此外, 考虑不等式

$$\frac{1}{(a_{k+1}+2)\cdot q_k^2}<\left|\xi^{(i_0)}-\frac{p_k}{q_k}\right|\leqslant\frac{C_1}{|Y|^n}\leqslant\frac{C_1}{|q_k|^n},$$

a_{k+1} 与 q_k 相比必须充分大, 即

$$a_{k+1}>\frac{|q_k|^{n-2}}{C_1}-2. \tag{8·13}$$

此不等式易于检验对所有 k 满足 $q_k\leqslant C$.

综上, 我们提出下面程序: 对 $i_0=1,\cdots,s$ 的每一个实根 $\xi^{(i_0)}$(注意 i_0 事先不知道), (1)计算 $\xi^{(i_0)}$ 的一个有理逼近 $\bar{\xi}$ 满足(8·12)(截取其十进表示式). (2)将 $\bar{\xi}$ 展开成它的具有部分商 $a_0, a_1, a_2, \cdots, a_{k+1}$ 的连分数且对满足 $q_k\leqslant C\leqslant q_{k+1}$ 的所有 i

$=1,\cdots k$，收敛于 p_i/q_i．(3)对条件(8·13)及 $F(p_i,q_i)=m$ 检验所有这些收敛．关于这一最后检验，注意到若 $X/Y=p_i/q_i$，则对满足 $z^n|m$ 的某个 $Z\in\mathbb{Z}$，$X=Z\cdot p_i$，$Y=Z\cdot q_i$．这一简单观察一般把大多数可约的商排除在外，且当 m 是第 n 个非幂整数时则是全部排除．

在 $|Y|\leqslant C$ 的范围内已检验所有解，我们可假定 $|Y|>C$．对于这样的解(X,Y)我们可得到与 A 对应的下界如下(其思想应归于 A. Pethö，也参见 Blass, Glass, Meronk 和 Steiner[18]第 1 节)．对每个$(i,j)\in\{1,\cdots,r\}\times\{1,\cdots,n\}$，设 φ_{ij}对这个$|\varepsilon_i^{(j)}|^{\varphi_{ij}}\geqslant 1$ 是数 $+1$ 或 -1，并设 $E_j=\prod_{i=1}^{r}|\varepsilon_i^{(j)}|^{\varphi_{ij}}$．则

$$|\beta^{(j)}|=|\mu^{(j)}|\cdot\prod_{i=1}^{r}|\varepsilon_i^{(j)}|^{a_i}\leqslant\mu_+\cdot E_j^A.$$

因此对满足 $j_1\neq j_2$ 的任意一对 j_1,j_2，有

$$|Y|=\frac{|\beta^{(j_1)}-\beta^{(j_2)}|}{|\xi^{(j_1)}-\xi^{(j_2)}|}\leqslant\mu_+\cdot\frac{E_{j_1}^A+E_{j_2}^A}{|\xi^{(j_1)}-\xi^{(j_2)}|},$$

而由此我们可找到 A 的一个下界，若我们已知$|Y|>C$的话．当然，对另一对 j_1,j_2 我们可找到一个不同的下界，因此可以取较大的一个．

8·5 应用：三角数是三个连续数的积

作为前节叙述的一般理论的应用，本节我们证明下面结果，问题已由 Mohanty 提出(参考 Mohanty[85]，此文中的证

明是错误的). 第 n 个三角数对 $n \in N$ 定义为 $T_n = \frac{1}{2} \cdot n \cdot (n+1)$.

定理 是三个连续整数之积的仅有三角数是 $T_3 = 1 \cdot 2 \cdot 3$, $T_{15} = 4 \cdot 5 \cdot 6$, $T_{20} = 5 \cdot 6 \cdot 7$, $T_{44} = 9 \cdot 10 \cdot 11$, $T_{608} = 56 \cdot 57 \cdot 58$, $T_{22736} = 636 \cdot 637 \cdot 638$.

证明 我们有丢番图方程 $n \cdot (n+1) = 2 \cdot m \cdot (m+1)(m+2)$, 其中 $n, m \in N$. 令 $x = 2 \cdot m + 2$, $y = 2 \cdot n + 1$. 则我们导出方程 $y^2 = x^3 - 4 \cdot x + 1$, 其中 $x, y \in N$, 满足 $x \geqslant 4$ 的偶数, $y \geqslant 3$ 的奇数. 现在, 由下面定理 8·7 来完成本文定理的证明.

定理 8·7 椭圆曲线

$$y^2 = x^3 - 4 \cdot x + 1 \tag{8·14}$$

仅有下面 22 个整数点:

$(x, \pm y) = (-2, 1), (-1, 2), (0, 1), (2, 1), (3, 4), (4, 7), (10, 31), (12, 41), (20, 89), (114, 1217), (1274, 45473)$.

证明此定理的两个主要步骤: 首先将此问题简化成解两个四次 Thue 方程. 然后运用产生于前节的一般理论解方程.

设 L 是全实域 $Q(\psi)$, 其中

$$\psi^3 - 4 \cdot \psi + 1 = 0.$$

令 ψ 的共轭是 $\psi^{(1)} = 0.254\cdots$, $\psi^{(2)} = -2.114\cdots$, $\psi^{(3)} = 1.860\cdots$. 由 Delone 和 Faddeev[35]的表我们看出 L 的类数是 1, 其整环是 $Z[\psi]$, 其判别式是 229, 而独立单位对是 $\psi, 2-\psi$. 由 Buchmann[27]的表 I 看 $-7+2 \cdot \psi^2$, $2 \cdot \psi + \psi^2$ 是 $Z[\psi]$中的基本单位对. 由 $-7+2 \cdot \psi^2 = -\psi^{-1} \cdot (2-\psi)$, $2 \cdot \psi + \psi^2 = (2-\psi)^{-1}$ 我

们看出 $\psi, 2-\psi$ 也是 $Z[\psi]$中的基本单位对.

椭圆曲线方程(8·14)可写成

$$y^2=(x-\psi)\cdot(x^2+x\cdot\psi+(\psi^2-4)) \qquad (8\cdot 15)$$

右边的因子是互素的.实际上,若 π 是其素公约数,则 π 将除尽

$$(x^2+x\cdot\psi+(\psi^2-4))-(x+2\cdot\psi)\cdot(x-\psi)$$
$$=3\cdot\psi^2-4,$$

这些是素数,因为其范数是 -229. 因此我们得到 π 是这素数的单位次,然后由(8·15), $x-\psi=$ 单位 $\times(3\cdot\psi^3-4)\times$ 平方. 取范数,则得 $y^2=\pm 229\times$ 平方,这显然不可能.

现在,(8·15)蕴涵

$$x-\psi=\pm\psi^i\cdot(2-\psi)^j\cdot\alpha^2,\ \alpha\in Z[\psi],$$
$$i,j\in\{0,1\}. \qquad (8\cdot 16)$$

因为(8·14)对解 $x\leqslant 0$ 是平凡的(满足 $x\leqslant 0$ 的仅有的解是列在定理中的前三对),我们可假定 $x\geqslant 1$. 因为 $\psi^{(1)}=0.254\cdots$, 我们看出(8·16)中的负号是不可能的. 则由 $\psi^{(2)}=-2.114\cdots$, $i\neq 1$. 我们因此断定

$$x-\psi=(2-\psi)^{(j)}\cdot(u+v\cdot\psi+w\cdot\psi^2)^2,$$
$$u,v,w\in Z, j\in\{0,1\} \qquad (8\cdot 17)$$

情形一：$j=0$，则蕴涵着(8·17)两边对应系数相等.

$$x=u^2-2\cdot v\cdot w,\ \ w^2-2\cdot u\cdot v-8\cdot v\cdot w=1,$$

$$v^2+4\cdot w^2+2\cdot u\cdot w=0 \qquad (8\cdot 18)$$

注意 w 是奇数，v 是偶数，因此 $4|2\cdot u\cdot w$，所以 u 是偶数. 令 $u=2u_1$，$v=2\cdot v_1$. (8·18)最后 1 个方程写成

$$w^2+u_1\cdot w+v_1^2=0.$$

作为 w 的二次方程来考虑，它的判别式必为一个平方数. 比如 z^2. 则

$$u_1^2-4v_1^2=z^2,\ \ w=\frac{1}{2}(-u_1+z).$$

注意 u_1 和 z 有相同的奇偶性. 我们可假定 $u\geqslant 0$.

首先假定 u_1 和 z 是偶数. 因为 $w^2+u_1\cdot w+v_1^2=0$ 以及 w 是奇数，我们发现 $u_1\equiv 2(\mathrm{mod}\,4)$ 且 v_1 是奇数. 令 $u_1=2\cdot u_2$，$z=2\cdot z_1$. 则 $u_2^2-v_1^2=z_1^2$，其中 u_2 和 v_1 是奇数. 由 $u_2\geqslant 0$，存在 $m,n\in Z$ 使得

$$u_2=m^2+n^2,\ \ v_1=m^2-m^2,\ \ z_1=2\cdot m\cdot n.$$

由此导出

$$u=4\cdot(m^2+n^2),\ \ v=2\cdot(m^2-n^2),\ \ w=-(m\pm n)^2.$$

因为 z 的符号. 由此 n 的符号并不重要，我们可假定 $w=-(m+n)^2$. 在(8·18)的第二个方程的代换之后，我们得 Thue 方程

$$m^4+36\cdot m^3\cdot n+6\cdot m^2\cdot n^2-28\cdot m\cdot n^3+n^4=1.$$

左边可分解成为

$$(m+n)\cdot(m^3+35\cdot m^2\cdot n-29\cdot m\cdot n^2+n^3),$$

因此很容易解. 其仅有的解是 $\pm(m,n)=(1,0),(0,1)$. 这导出 $\pm(u,v,w)=(4,2,-1),(4,-2,-1)$, 则由(8·18), 我们分别找到 $x=20,12$, 这提供(8·14)的解 $(x,\pm y)=(20,89),(12,41)$.

第二, 我们假定 u_1 和 z 是奇数. 则 v_1 是偶数, 因此由 $u_1\geqslant 0$, 存在 $m,n\in Z$ 满足

$$u_1=m^2+n^2,\ 2\cdot v_1=2\cdot m\cdot n,\ z=m^2-n^2.$$

此导出

$$u=2\cdot(m^2+n^2),\ v=2\cdot m\cdot n,\ w=-m^2 \text{ 或 } w=-n^2.$$

我们可假定 $w=-m^2$. 将其代换(8·18)中第 2 个方程, 我们得 Thue 方程

$$m^4+8\cdot m^3\cdot n-8\cdot m\cdot n^3=1.$$

其左边可以再简化. 容易看出, 仅有的解是 $\pm(m,n)=(1,0),(1,1),(1,-1)$. 因为 m 和 n 不能有相同的奇偶性, 仅认可第一对解. 这就导出 $(u,v,w)=(2,0,-1)$, 因此对(8·14), 得 $(x,\pm y)=(4,7)$.

情形二: $j=1$. 此时(8·17)中系数相等, 得

$$x=2\cdot u^2+v^2+4\cdot w^2+2\cdot u\cdot w-4\cdot v\cdot w, \tag{8·19}$$

$$\begin{cases} u^2+4\cdot v^2+18\cdot w^2-4\cdot u\cdot v+8\cdot u\cdot w-18\cdot v\cdot w=1, \\ 2\cdot v^2+9\cdot w^2-2\cdot u\cdot v+4\cdot u\cdot w-8\cdot v\cdot w=0 \end{cases} \tag{8·20}$$

(8·20)的第一个关系式可用

$$u^2-2\cdot v\cdot w=1 \tag{8·21}$$

代换. 注意 u 是奇数. 设 $z=v-2\cdot w$. 则(8·20)第 2 个方程导出

$$w^2=2\cdot z\cdot(u-z).$$

首先假定 2 是奇数, 则存在 $m,n\in Z$ 使得

$$z=m^2,\ u-z=2\cdot n^2,$$

这里我们用到 $u\geqslant 0$ 和 $(u,w)=1$. 因此, 选择适当的符号,

$$u=m^2+2\cdot n^2,\ v=m^2+4\cdot m\cdot n,\ w=2\cdot m\cdot n.$$

将其代入(8·21)中, 得方程

$$m^4-4\cdot m^3\cdot n-12\cdot m^2\cdot n^2+4\cdot n^4=1. \tag{8·22}$$

在定理 8·8(i)之下我们证明这方程仅有解 $\pm(m,n)=(1,0)$, 导出 $(u,v,w)=(1,1,0)$, 最后, 对(8·14)得 $(x,\pm y)=(3,4)$.

第二, 我们假定 z 是偶数. 则存在 $m,n\in Z$ 满足

$$z = 2 \cdot m^2,\ u - z = n^2.$$

因此选择适当的符号，我们发现

$$u = 2 \cdot m^2 + n^2,\ v = 2 \cdot m^2 + 4 \cdot m \cdot n,\ w = 2 \cdot m \cdot n.$$

现在，代入(8·21)，得 Thue 方程

$$n^4 - 12 \cdot n^2 \cdot m^2 - 8 \cdot n \cdot m^3 + 4 \cdot m^4 = 1. \qquad (8 \cdot 23)$$

依据定理 8·8(ii)，我们证明这方程仅有解 $\pm(m, n) = (0, 1)$, $(1, -1)$, $(3, 1)$, $(-1, 3)$. 他们分别导出了 $(u, v, w) = (1, 0, 0)$, $(3, -2, -2)$, $(19, 30, 6)$, $(11, -10, -6)$，这导出(8·14)的解 $(x, \pm y) = (2, 1)$, $(10, 31)$, $(1274, 45473)$, $(114, 1217)$. 因此，此结果完成了定理 8·7 的证明，这是以方程(8·22)、(8·23)仅有解对 (m, n) 作为条件的，已如上述. 现在我们着手证明这一点.

定理 8·8 (i) Thue 方程

$$X^4 - 4 \cdot X^3 \cdot Y - 12 \cdot X^2 \cdot Y^2 + 4Y^2 = 1 \qquad (8 \cdot 24)$$

仅有解 $\pm(X, Y) = (1, 0)$.

(ii) Thue 方程

$$X^4 - 12 \cdot X^2 \cdot Y^2 - 8 \cdot X \cdot Y^3 + 4 \cdot Y^4 = 1 \qquad (8 \cdot 25)$$

仅有解 $\pm(X, Y) = (1, 0)$, $(1, -1)$, $(1, 3)$, $(3, -1)$.

证明 采用8·3节和8·4节的记号和结果. 设代数数 θ 和 φ 由

$$\theta^4 - 12\cdot\theta^2 - 8\cdot\theta + 4 = 0, \varphi^4 - 4\cdot\varphi^3 - 12\cdot\varphi^2 + 4 = 0$$

定义. 因为 $\varphi = 2/\theta$, 这导出 θ 和 φ 生成 Q 上的相同域 K. 在8·2节的记号之下, 我们有 $n = 4, s = 4, t = 0$ 和 $\xi = 0$ 或 $\xi = \varphi$. 简单的计算表明, 对 $\xi = \theta, \varphi$, 我们能取

$$Y_0 = 1, C_1 = 0.843, C_2 = 0.589, Y_1 = 2, C_3 = 6.645,$$
$$Y_2^* = 3, \mu_- = \mu_+ = 1, C_4 = 8.3374.$$

在这些运算中, 我们从上面估计 C_1, C_3, C_4 并从下面估计 C_2, 用下面对 θ 和 φ 的共轭的逼近:

$$\theta^{(1)} \cong -1.080\,286\,352, \quad \varphi^{(1)} \cong -1.851\,360\,980,$$

$$\theta^{(2)} \cong 3.722\,935\,260, \quad \varphi^{(2)} \cong 0.537\,210\,524,$$

$$\theta^{(3)} \cong 0.334\,111\,716, \quad \varphi^{(3)} \cong 5.986\,021\,747,$$

$$\theta^{(4)} \cong -2.976\,760\,624, \quad \varphi^{(4)} \cong -0.671\,871\,290.$$

现在我们引入 K 满足 Z－基 $\{1, \theta, \frac{1}{2}\cdot\theta^2, \frac{1}{2}\cdot\theta^3\}$ 的阶 R(注意到 $\frac{1}{2}\cdot\theta^2$ 是一个代数整数). 注意

$$\varphi = \frac{2}{\theta} = 4 + 6\cdot\theta - \frac{1}{2}\cdot\theta^3 \in R.$$

另一方面，(8·24)和(8·25)分别等价于 $\mathrm{Norm}_{K/Q}(X - Y\cdot\theta) = 1$ 和 $\mathrm{Norm}_{K/Q}(X - Y\cdot\varphi) = 1$，这意味着若$(X,Y)$是(8·24)或者(8·25)的解，则 $X - Y\cdot\theta$ 或者 $X - Y\cdot\varphi$ 分别是阶 R 的单位. R 的一个基本单位组由

$$\varepsilon_1 = 1 + \theta,\ \varepsilon_2 = 3 + \theta,\ \varepsilon_3 = \frac{1}{2}\cdot\theta^2$$

给出. 这里我们不证明这一事实. 关于其证明，看 Tzanakis 和 de Weger[124]，第Ⅲ.2 节及附录Ⅰ.

因此(8·24)和(8·25)的解简化为导出所有$(a_1, a_2, a_3) \in Z^3$，使得单位 $\pm\varepsilon_1^{a_1}\cdot\varepsilon_2^{a_2}\cdot\varepsilon_3^{a_3}$ 分别有特别的形状 $X - Y\cdot\theta$ 或 $X - Y\cdot\varphi$. 采用引理 8·3 的记号，在一些数值计算之后，我们留给读者去检验，我们有

$$\min_I N[U_I^{-1}] = 0.634950\cdots,$$

$$\max_I N[U_I^{-1}] = 1.210070\cdots.$$

(当然，这儿 $I = \{1,2,3,4\}$). 因此在引理 8·4 中我们可取

$$C_5 = 1.211.$$

也有

$$C_6 = 6.38771\times10^4,\ Y_2' = 3.$$

(C_5 和 C_6 的值由上述来估计).

现在，对我们的情形，关系式(8·3)变成

$$\Lambda = \log \left| \frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \right| + \sum_{i=1}^{3} a_i \cdot \log \left| \frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}} \right|, \tag{8·26}$$

其中 $\xi = \theta$ 或 φ. 如 8·2 节所述，固定一次 i_0，我们可检验任意的 j, k. 因此我们能检验

$$\begin{cases} j = 3, k = 4, \text{若 } i_0 = 1 \text{ 或 } 2, \\ j = 1, k = 2, \text{若 } i_0 = 3 \text{ 或 } 4. \end{cases} \tag{8·27}$$

因此，对每个 $\xi \in \{\theta, \varphi\}$，$\Lambda$ 有四种可能. 对于每一个这样的八种情形，正如我们下面要证明的，有

$$C_7 = 5.71 \times 10^{38}, \ C_8 = 6.17,$$

由此，用引理 8·3，若 $|Y| > 3$，则对 $A = \max_{1 \leq i \leq 3} |a_i|$，有上界 $C_9 = 3.26 \times 10^{40}$. 照此易于检验，(8·24) 或 (8·25) 满足 $|Y| \leq 3$ 的仅有的解已在定理的陈述中列出. 因此我们可假定 $|Y| > 3$，因此

$$A < 3.26 \times 10^{40}.$$

在我们应用 3·8 节的简化方法之前，我们证明引理 2·4 的应用导出上述常数 C_7, C_8. 我们将此结果应用于由 (8·26) 给出的 Λ 的情形. 在此情形，我们对出现于 Λ 中的各个不同的 a_i，计算 V_i 如下. 若 $\alpha_i = |\varepsilon_i^{(k)}/\varepsilon_i^{(j)}|$，$i = 1, 2, 3$，则 α_i 是单位而由此 a_0（出现在 $h(\alpha_i)$ 的计算中）等于 1. 显然，α_i 的每一个共轭的绝对值比

$$H_i = \frac{\max\limits_{1\leqslant h\leqslant 4}|\varepsilon_i^{(h)}|}{\min\limits_{1\leqslant h\leqslant 4}|\varepsilon_i^{(h)}|}$$

小．且 $H_i \geqslant 1$．因此 $h(\alpha_i) \leqslant H_i$，我们能取

$$V_i = \max[\log H_i, |\log|\varepsilon_i^{(k)}/\varepsilon_i^{(j)}||].$$

因为后项等于 $|\varepsilon_i^{(k)}/\varepsilon_i^{(j)}|$ 或它的逆的对数，导出

$$V_i = \log H_i.$$

若 $\alpha_i = |\xi^{(i_0)} - \xi^{(j)}| / |\xi^{(i_0)} - \xi^{(k)}|$，则 α_i 的所有共轭的绝对值比 C_3 小．因此，$h(\alpha_i) \leqslant (\log a_0)/d + \log C_3$，其中 a_0 和 d 如同在 $h(\alpha)$ 对 $\alpha = \alpha_i$ 的定义中．a_0 的一个上界可作如下计算．对 $i, h \in \{1, \cdots, 4\}$ 连同 $i \neq h$，考虑代数数 $\chi_{ih} = \frac{1}{2}\cdot(\xi^{(i)} - \xi^{(h)})$．可检验，对 $\xi = \theta$ 或 φ，数 χ_{ih} 是代数整数．现在，对每个置换 $\sigma = (\sigma_1\sigma_2\sigma_3\sigma_4) \in S_4$，我们考虑数 $\chi(\sigma) = \chi_{\sigma_1\sigma_2}/\chi_{\sigma_1\sigma_3}$（不依赖 σ_4）及多项式

$$P(X) = \prod_{\sigma \in S_4}[X - \chi(\sigma)]$$

也考虑数

$$\Delta = \prod_{1\leqslant i<h\leqslant 4}\chi_{ih}$$

注意

$$\Delta^2 = \frac{1}{2^{12}}\cdot\prod_{1\leqslant i<h\leqslant 4}(\xi_i - \xi_h)^2 = \frac{1}{2^{12}}\cdot D$$

其中 D 是 ξ 的定义多项式的判别式，因此 $\Delta^2 = 229$．另一方

面，$P(X)$的系数适合于$\chi(\sigma)$对$\sigma\in S_4$的基本对称函数的符号，因此，它们是具有有理系数的$\xi^{(i)}$的对称表达式.这意味着$P(X)\in Q[X]$.另一方面，由Δ的定义，$P(X)$的系数乘以Δ^4是χ_{ih}的多项式，满足系数在Z中从而是代数整数.结合这些以及$P(X)\in Q[X]$的事实可看出$229^2\cdot P(X)\in Z[X]$.因此，由于α_i是$P(X)$的根，其首项系数a_0至多是229^2.最后，我们有$h(\alpha_i)\leqslant 2\cdot(\log 229)/d+\log C_3$以及明显有$|\log\alpha_i|/d\leqslant\log C_3$.因为$\alpha_i\overline{\in}Q$，我们有$d\geqslant 2$，故可取

$$V_i=\log 229+\log C_3.$$

现在，简单计算表明

$$\log H_1=4.074586\cdots,\quad \log H=5.667432\cdots,$$

$$\log H_3=4.821584\cdots,$$

$$\log C_3=1.262065\cdots,\quad \text{当 } \xi=\theta \text{ 时},$$

$$\log C_3=1.893823\cdots,\quad \text{当 } \xi=\varphi \text{ 时},$$

$$\log 229+\log C_3\leqslant 7.327545\cdots.$$

因此，我们对$n=4, D\leqslant 24, e(n)=73$应用引理2·4

$$\alpha_1=\left|\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}\right|,\quad \alpha_2=\left|\frac{\varepsilon_3^{(k)}}{\varepsilon_3^{(j)}}\right|,\quad \alpha_3=\left|\frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}}\right|,$$

$$\alpha_4 = \left| \frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \right|,$$

对 $\xi = \theta$ 或 φ, 以及 $b_1 = a_1, b_2 = a_3, b_3 = a_2, b_4 = 1, B = A, V_1 = \log H_1, V_2 = \log H_3, V_3 = V_3^+ = \log H_2, V_4 = V_4^+ = \log 229 + \log C_3$. 因此, 我们找到

$$|\Lambda| > \exp[-C_7 \cdot (\log A + C_8)],$$

满足 $C_7 = 5.71 \times 10^{38}$ 及 $C_8 = 6.17$.

现在我们应用 3·7 节中所述的简化程序. 在我们的情形与解(8·9)有关

$$K_1 = C_6 = 6.38771 \times 10^4, \quad K_2 = \frac{n}{C_5} = \frac{4}{1.211} > 3.303,$$

$$K_3 = 3.26 \times 10^{40}.$$

(K_2 由下面估计), 又

$$\Lambda = \delta + a_1 \cdot \mu_1 + a_2 \cdot \mu_2 + a_3 \cdot \mu_3$$

这里对 δ 和 μ_i, 由(8·26)和(8·27)的观察, 有

$$\begin{cases} \delta = \delta_1 := \log \left| \dfrac{\xi^{(1)} - \xi^{(3)}}{\xi^{(1)} - \xi^{(4)}} \right| \text{ 或 } \delta = \delta_2 := \log \left| \dfrac{\xi^{(2)} - \xi^{(3)}}{\xi^{(2)} - \xi^{(4)}} \right|, \\ \mu_i = \log \left| \dfrac{\varepsilon_i^{(4)}}{\varepsilon_i^{(3)}} \right|, \text{对 } i = 1, 2, 3, \end{cases}$$

其中 $\xi = \theta$ 或 φ (8·28)

或

$$\begin{cases}\delta=\delta_3:=\log\left|\dfrac{\xi^{(3)}-\xi^{(1)}}{\xi^{(3)}-\xi^{(2)}}\right| \text{ 或 } \delta=\delta_4:=\log\left|\dfrac{\xi^{(4)}-\xi^{(1)}}{\xi^{(4)}-\xi^{(2)}}\right|, \\ \mu_i=\log\left|\dfrac{\varepsilon_i^{(2)}}{\varepsilon_i^{(1)}}\right|, \text{对 } i=1,2,3,\end{cases}$$

其中 $\xi=0$ 或 φ (8·29)

详细数值在 Tzanakis 和 de Weger[124]中列出. 我们取 $C_0=10^{140}$, 并着手于满足联合矩阵

$$\mathfrak{S}=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ [C_0\cdot\mu_1] & [C_0\cdot\mu_2] & [C_0\cdot\mu_3]\end{bmatrix}$$

的格. 注意在(8·28)(分别地, (8·29)的四种情形的每一种, 我们有相同的格, 比如说 Γ_1(分别地, Γ_2). 在每一种 $\delta\neq0$ 的情形, 我们没有关于 μ_i 是 Q－相关的数值依据. 因此我们按 8·4 节情形(ii)来做.

对每个 Γ_i 我们已应用 L^3－运算的整数形式, 每一次我们计算整数的 3×3 矩阵 $\mathscr{B}, \mathscr{U}, \mathscr{U}^{-1}$, 如 3·7 节所定义的. 在我们的情形, 简化基(即 $\mathscr{B}$ 的元素)向量的坐标产生 46 至 48 个数字, 即简化基向量的长的大小以 $C_0^{1/3}$ 作为期望值. 对八种情形的每一种, 我们计算

$$\underline{x}=\begin{bmatrix}0\\ 0\\ -[C_0\cdot\delta]\end{bmatrix}$$

关于格的简化基 $\underline{b}_1, \underline{b}_2, \underline{b}_3$ 的坐标 s_1, s_2, s_3. 由计算, 我们找到

$$|\underline{b}_1|>3.247\times10^{46}, \text{在格 } \Gamma_1 \text{ 的情形},$$

$$|\underline{b}_1|>4.846\times10^{46}$$，在格 Γ_2 的情形，

$$\|s_3\|>0.029$$，在所有 8 种情形.

观察引理 3·5，这意味着在所有情形 $i_0=3$，且

$$\iota(\Gamma_i,\underline{x})>0.029\cdot\frac{1}{2}\cdot3.247\times10^{46}>4.708\times10^{44}.$$

则引理 3·10 的假设完全满足 $n=3$，$r=1$，$C=c_0$，$c=K_1$，$\delta=K_2$，$X_0=X_1=K_3$，因为 $\sqrt{27}\cdot K_3<1.112\times10^{40}$，此蕴涵

$$\begin{aligned}A&<\frac{1}{3.303}\cdot\log[10^{140}\cdot6.38771\times10^4/3.26\times10^{40}]\\&<72.8.\end{aligned}$$

这导出 $A\leqslant72$. 我们对 $K_3=72$ 及 $c_0=10^{12}$ 重复此程序. 由计算，找到

$$|\underline{b}_1|>1.293\times10^4$$，在格 Γ_1 的情形，

$$|\underline{b}_1|>1.092\times10^4$$，在格 Γ_2 的情形，

$$\|s_3\|>0.143$$，在所有 8 种情形.

观察引理 3·5，这意味着在所有情形 $i_0=3$，且

$$\iota(\Gamma_i,\underline{x})>0.143\cdot\frac{1}{2}\cdot1.092\times10^4>7.807\times10^2.$$

则引理 3·10 的假设完全满足，因为 $\sqrt{27}K_3<3.742\times10^2$，这

蕴涵

$$A < \frac{1}{3.303} \cdot \log[10^{12} \cdot 6.38771 \times 10^4 / 72] < 10.5.$$

这导出 $A \leqslant 10$. 我们枚举所有剩下的可能，没有找到(8·24)和(8·25)的所述之外的其他解.

证明定理 8·8 的计算用 35 秒.

8·6 Thue－Mahler 方程，简述

设 $F(X, Y)$ 如 8·1 节中所述. 设 $p_1, \cdots, p_s$ 是固定的不同素数. 丢番图方程

$$F(X, Y) = \pm \prod_{i=1}^{s} p_i^{n_i},$$

其中变量 $X, Y \in \mathbb{Z}$, $n_1, \cdots, n_s \in \mathbb{N}_0$, $(X, Y) = 1$, 称为 Thue－Mahler 方程. Mahler[73]已证明此方程仅有有限多个解，Coates[33]已证明这些解能够、至少在主部上能够有效确定，因为变量的有效可计算的上界能由 p－adic 对数线性型理论导出. 关于此方程的历史我们参考 Shorey 和 Tijdeman[107]，第 7 章.

我们相信，不仅是在主部，而是在实际上解 Thue－Mahler 方程是可能的. 做法是基于对格的简化基的 L^3－运算. 使用实的和 p－adic 计算的丢番图逼近相结合的方法，降低上述上界(参考 3·7 和 3·8 节关于实的情形，3·11 和 3·12 节关于 p－adic 情形，1·5 节关于实的和 p－adic 的方法如何结合的简述，以及 4·8 和 6·4 节关于这种结合的方法的一些

详述的例子). 可考虑这样的方法:前几节关于解 Thue 方程的方法作为 p-adic 模拟.

这样一种思想(但没有用 L^3 - 运算)已被 Agrawal, Coates, Hunt 和 Van der Poorten 采用,就是解方程

$$X^3 - X^2 \cdot Y + X \cdot Y^2 + Y^3 = \pm 11^n.$$

据作者所知,这仅是文献中的例子,其中 Thue - Mahler 方程已用 Gelfond - Baker 方法解决. 其他方法也可用于解 Thue - Mahler 方程. 例如

$$X^3 + 3 \cdot Y^2 = 2^n$$

已由 Tzanakis[122]用不同方法解决. 上面许多其他想法的 Gelfond- Baker 方法的优点是在主部方面可用于任意的 Thue - Mahler 方程,因为我们想解决的特殊方程不怎么依赖于参量.

上述两个例子的 Thue - Mahler 方程是最简单的类型,实际观察三次域 $Q(\theta)$,其中 θ 是 $F(X,1)=0$ 的一个根,仅有一个基本单位,仅产生一个素数. 因此,运用二维实连分数及一维 p-adic 连分数就足够了,以代替复杂的 L^3 - 运算(1980 年,当 Agrawal, Coates, Hunt 和 van der Poorten 进行他们的工作时,这种运算的任何方法仍不是有效的). 适合运用 L^3 - 运算的方法在主部上可扩充到一般情况,其中有多于一个的基本单位及多于一个的素数. 有关这方面的工作可参见文献[125],[137].

参考文献

[1] Agrawal, M. k Coates, J. H., Hunt, D. C. and van der Poorten, A. J., Elliptic curves of conductor 11, Math. Comp. 35 (1980), 991 - 1002

[2] Alex, L. J., Diophantine equations related to finite groups, Comm. Algebra 4 (1976), 77 - 100

[3] Alex, L. J., On the diophantine equation $1 + 2^a = 3^b5^c + 2^d3^e5^f$, Math. Comp. 44 (1985a), 267 - 278

[4] Alex, L. J., On the diophantine equation $1 + 2^a = 3^b7^c + 2^d3^e7^f$, Arch. Math. 45 (1985b), 538 - 545

[5] Babai, L., On lovasz lattice reduction and the nearest lattice point Problem, Combinatorica 6 (1986), 1 - 13

[6] Bachman, G., Introduction to p - adic Numbers and Valuation Theory, Academic Press, New York and London (1964)

[7] Baker, A., Linear forms in the logarithms of algebraic numbers, Mathematika 13 (1966), 204 - 216

[8] Baker, A., Contributions to the theory of diophantine equations, I, On the Representation of integers by binary forms, II, the diophantine equation $y^2 = x^3 + k$, Phil. Trans. R. Soc. London, A 263 (1968), 173 - 208

[9] Baker, A., A sharpening of the bounds for linear forms in logarithms I, Acta Arith. 21 (1972), 117 - 129

[10] Baker, A., The theory of linear forms in logarithms, Tran-

scendence Theory: Advances and Applications, A. Baker (ed.), Academic Press, London (1977), 1 – 27

[11]Baker, A. and Davenport, H., The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = x^2$, Q. Jl. Math. Oxford (2) 20 (1969), 129 – 137

[12]Baker, A. and Wüstholz, G., Logarithmic forms and group varieties, J. Reine Angew. Math., 442 (1993), 19 – 62

[13]Berwick, W. E. H., Algebraic number fields with two independent units, Proc. London Math. Soc. 34 (1932), 360 – 378

[14]Beukers, F., On the generalized Ramanujan – Nagell equation, Acta Arith. Ⅰ: 38; Ⅱ: 39 (1981), 389 – 410; 113 – 123

[15]Billevič, K. K., On the units of algebraic fields of third and fourth degree (Russian), Mat. Sbornik Vol. 40, 82 (1956), 123 – 137

[16]Billevič, K. K., A theorem on the units of algebraic fields of n – th degree (Russian), Mat. Sbornik Vol. 64, 106 (1964), 145 – 152

[17]Blass, J., Glass, A. M. W., Meronk, D. B. and Steiner, R. P., Practical Solutions to Thue equations of degree 4 over the rational integers, Preprint, Bowling Green State Vniversity (1987ª)

[18]Blass, J., Glass, A. M. W., Meronk, D. B. and Steiner, R. P., Practical Solutions to Thue equations over the rational integers, Preprint, Bowling Green State Vniversity

(1987^b)

[19] Blass, J., Glass, A. M. W. Manski, D. K. Meronk, D. B. and Steiner, R. P., Constants for lower bounds for linear forms in the logarithms of algebraic numbers I: The general case, Preprint, Acta Arith. 55 (1990), 1 – 14

[20] Blass, J., Glass, A. M. W, Manski, D. K., Meronk, D. B. and Steiner, R. P., Constants for lower bounds for linear forms in the logarithms of algebraic numbers II: The homogeneous rational case, Acta Arith. 55 (1990), 15 – 22

[21] Borevich, Z. I. and Shafarevich, I. R., Number Theory, Academic Press, New York (1966)

[22] Bremner, A., Calderbank, R., Hanlon, P., Morton, P. and Wolfskill, J., Two – weight ternary codes and equation $y^2 = 4 \times 3^a + 13$, J. Number Theory 16 (1983), 212 – 234

[23] Brenner, J. L. and Foster, L. L., Exponential diophantine equations, Pacific J. Math. 101 (1982), 263 – 301

[24] Brent, R. P., A Fortran multiple – precision arithmetic package, ACM Trans. Math. Software 4, 57 – 70; and: Algorithm 524. MP, a Fortran multiple – precision arithmetic package, ACM Trans. Math. Software 4, 71 – 81 (1978)

[25] Brentjes, A. J., Multi – dimensional Continued Fraction Algarithms, MC Tract 145, Centr. Math. Comput. Sci., Amsterdam (1981)

[26] Brown, E., Sets in which xy + k is always a square, Math. Comp. 45 (1985), 613 – 620

[27]Buchmann, J., The generalized Voronoi – algorithm in totally real algebraic number fields, Proceedings EUROCAL' 85, Linz, Austria, Vol. 2, Lecture Notes in Comput. Sci. 204, Springer Verlag, Berlin (1985), 479 – 486

[28] Buchmann, J., A generalization of Voronoi's unit algorithm I& II, J. Number Theory 20 (1986), 177 – 191&192 – 209

[29] Bugeaud, Y. and Györy, K., Bounds for the solutions of Thue – Mahler equations and norm form equations, Acta Arith., 74(1996), 273 – 292

[30]Cassels, J. W. S., An Introduction to Diophantine Approximation, Cambridge Vniversity Press, Cambridge (1957)

[31]Cherubini, J. M. and Walliser, R. V., On the computation of all imaginary quadratic fields of class number one, Math. Comp. 49 (1987), 295 – 300

[32] Coates, J. An effective p – adic analogue of a theorem of Thue, Acta Arith. 15 (1969), 279 – 305

[33] Coates, J. An effective p – adic analogue of a theorem of Thue, II : The greatest prime factor of a binary form, Acta Arith. 16 (1970), 399 – 412

[34]Cohen, E. L., On the Ramanujan – Nagell equation and its generalizations, in: Number Theory (Banff, AB, 1988), pp. 81 – 92, de Gruyter, Berlin (1990)

[35] Delone, B. N. and Faddeev, D. K., The theory of irrationalities of the third degree, Transl. of Math. Monogr., Vol 10, A.M.S., Providence R.I. (1964)

[36]Elison, W.J., Recipes for solving diophantine problems by Baker's method, Sém. Théorie des Nombres, Vniversité de Bordeaux I, 1970 - 1, Lab. Th. Nombr. C. N. R. S., Exp. 12, 10pp. (1971a)

[37] Ellison, W.J., On a theorem of S. Sivasankaranarayana Pillai, Sém. Théorie des Nombres, Vniversité de Bordeaux I, 1970 - 1, Lab. Th. Nombr. C. N. R. S., Exp. 12, 10 pp. (1971b).

[38]Ellison, W.J., Ellison, F., Pesek, J. Stahl, C.E. and Stall, D.S., The diophantine equation $y^2 + k = x^3$, J. Number Theory 4 (1972), 107 - 117

[39]Evertse, J. - H., Vpper Bounds for the Numbers of Solutions of Diophantine Equations, MC Tract 168, Centr. Math. Comput. Sci., Amsterdam (1983)

[40] Evertse, J. - H., Györy, K., Stewart, C.L. and Tijdeman, R., S - unit equations and their applications, New advances in transcendence theory (Proc. Symp. Durham July 1986), A. Baker(ed.), Cambridge Vniversity Press, Cambridge (1988), 110 - 174

[41] Faltings, G., Endlichkeitssätze für abelsche Varietaten über Zahlkörpern, Invent. Math. 73 (1983), 349 - 366

[42]冯克勤,代数数论入门,上海科学技术出版社,上海,1988

[43]Fincke, U. and Pohst, M., Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, Mach. Comp. 44 (1985), 463 - 471

[44]Gaál, I., On the resolution of inhomogeneous norm form e-

quation in two dominating variables, Math. Comp. 51 (1988), 359 - 373

[45] Grinstead, C. M., On a method of solving a class of diophantine equations, Math. Comp. 32 (1978), 936 - 940

[46] Grosswald, E., Topics from the Theory of Numbers, 2nd. ed., Birkhäuser, Boston (1984)

[47] 郭永东, 丢番图方程 $1 + p^x = q^y + p^z \cdot q^w$, 广东省雷州师专学报自然科学版, 1989, (1)

[48] 郭永东, 丢番图方程 $1 + 2^x = 11^y + 2^z \cdot 11^w$ 的非平凡解, 广西师范大学学报自然科学版, 1990, (1)

[49] 郭永东, 关于丢番图不等式 $0 < KX - LY < (LY)^\delta$, 湛江师范学院学报自然科学版, 1994, (1)

[50] Guo, Y. - D., On the diophantione equation $x^2 = 2^{2a}k^{2m} - 2^{2a}k^{m+n} + 1$, Discuss. Math., 16(1996)

[51] Guo, Y. - D. and Le, M. - H., A note on Ješmanowiczconjecture concerning Pythagorean numbers, Commen. Math., 44 (1995), 225 - 228

[52] Guo, Y. - D. and Le, M. - H., A note on the diophantine equation $x^2 - 2^m = y^n$, Proc. Amer. Math. Soc., 123 (1995), 3627 - 3629

[53] Hardy, G. H. and Wright, E. M., An Introduction to the Theory of Numbers, (5th ed.), Oxford Vniversity Press, Oxford (1979)

[54] Hasse, H., Über eine diophantische Gleichung von Ramanujan - Nagell und ihre Verallgemeinerung, Nagoya Math. J. 27 (1966), 77 - 102

[55] Kiss, P., Zero terms in second order linear recurrences, Math. Sem. Notes Kobe Univ. (Japan) 7 (1979), 145 152

[56] Knuth, D. E., The Art of Computer Programming, Vol. 2: Seminumerical Algorithms, (2nd ed.), Addison – Wesley, Reading Mass. (1981)

[57] Koblitz, N., p – adic Numbers, p – adic Analysis, and Zeta – functions, Springer Varlag, New York (1977)

[58] Koblitz, N., p – adic Analysis: a Short Course on Recent Work, Cambridge University Press, Cambridge (1980)

[59] Koksma, J. F., Diophantische Approximationen, Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 4, Springer-Verlag (1937), 407 – 571

[60] Lagarias, J. C. and Odlyzko, A. M., Solving low – density subset sum Problems, J. Assoc. Comput. Mach. 32 (1985), 229 – 246

[61] Langevin, M. Quelques applications de nouoveaux résultats de van der Poorten, Sém. Delange – Pisot – Poitou 1975/76, Paris, Exp. G12, (1976)

[62] Laurent, M., Mignotte, M. and Nesterenko, Y., Formes linéares en deux logarithmes et déterminants d'interpolation, J. Number Theory 55 (1995), 285 – 321

[63] Le, M. – H., On the generalized Ramanujan – Nagell equation $x^2 - D = p^n$, Acta Arith. 58 (1991), 289 – 298

[64] Le, M. – H., On the number of solutions of the generalized Ramanujan – Nagell equation $x^2 - D = 2^{n+2}$, Acta

Arith. 60 (1991), 149 – 167

[65] Le, M. – H., On the generalized Ramanujan – Nagell equation $x^2 - D = 2^{n+2}$, Trans. Amer. Math. Soc. 334 (1992), 809 – 825

[66] 乐茂华, 关于指数型丢番图方程的整数解, 数学进展 23 (1994), 385 – 395

[67] Lehmer, D. H., On a problem of Störmer, Illinois J. Math. 8(1964), 57 – 79

[68] Lenstra, A. K., Polynomial – time Algorithms for the Factorization of Polynomials, Dissertation, University of Amsterdam (1984)

[69] Lenstra, A. K., Lenstra, H. W. Jr. and Lovász, L., Factoring polynomials with rational coefficients, Math. Ann. 261 (1982), 515 – 534

[70] Loxton, J. H., Mignotte, M., Van der Poorth, A. J. and Waldschmidt, M., A lower bound for linear forms in the logarithms of algebraic numbers, C. R. Math. rep. Acad. Sci. Xanada 11 (1987), 119 – 124

[71] Lutz, É., Sur les approximations diophantiennes linéaires p – adiques, Thése, Université de Strasbourg (1951)

[72] Macwilliams, F. J. and Sloane, N. J. A., The Theory of Error – Correcting Codes, North – Holland, Amsterdam (1977)

[73] Mahler, K., Zur Approximation algebraischer Zahlen I: Über den grössten Primteiler binärer Formen, Math. Ann. 107 (1933), 691 – 730

[74] Mahler, K., Eine arithmetische Eigenschaft der rekurrierenden Reihen, Mathematika B(Leiden) 3 (1934), 153 – 156

[75] Mahler, K., Über der grössten Primteiler spezieller Polynome zweiten Grades, Arch. Math. Naturvid. B 41 (1935), 3 – 26

[76] Mahler, K., Lectures on Diophantine Approximations I: g – adic Numbers and Roth's Theorem, University of Notre Dame Press, Notre Dame (1961)

[77] Masser, D. W., Open problems, proc. Symp. Analytic Number Th., W. W. L. Chan (ed.), London, Imperial Collgeg (1985)

[78] Mignotte, M., On the automatic resolution of certain diophantine equations, Proceedings of EUROSAM 84, Lecture Notes in Comput. Sci. 174, Springer Verlag, Berlin (1981^a), 378 – 385

[79] Mignotte, M., Une nouvelle résolution de l'équation $x^2 + 7 = 2^n$, Rend. Sem. Fac. Sci. Univ. Cagliari 54, Fasc. 2 (1984^b), 41 – 43

[80] Mignotte, M. $p(x^2 + 1) \geqslant 17$ si $x \geqslant 240$, C. R. Acad. Sci. Paris 301, Série I, No. 13 (1985), 661 – 664

[81] Mignotte, M. and Waldschmidt, M., Linear forms in two logarithms and Schneider's method, Math. Ann 231 (1978), 241 – 267

[82] Mignotte, M. and Waldschmidt, M., Linear forms in two logarithms and Schneider's method (Ⅱ), Acta. Arith. 53

(1989),250－287

[83]莫德译,具有四项的指数丢番图方程(Ⅱ),数学学报,37 (1994),482－490

[84]Mo, D. － Z. and Tijdeman, R., Exponential diophantine equations with four terms, Indag. Math. (N. S.), 3 (1992), 47－57

[85]Mohanty, S. P., Integer points of $y^2 = x^3 - 4x + 1$, J. Number Theory 30 (1988), 86－93

[86]Nagell, T., Løesing oppg. 2, 1943, S. 29 (Norwegian), Norsk Mat. Tidsskr. 30 (1948), 62－64

[87]Odlyzko, A. M. and te Riele, H. J. J., Disproof of the Mertens conjecture, J. reine angew. Math. 357 (1985), 138－160

[88]Oesterlé, J., Nouvelles approaches du Théoréme Fermat, Sem. Bourbaki, No. 694 (1987/88), 1－21

[89]潘承洞,潘承彪,初等代数数论,山东大学出版社,济南,1991

[90]Pethö, A., Full cubes in the Fibonacci sequence, Publ. Math. Debrecen 30 (1983), 117－127

[91]Pethö, A., On the solution of the diophantine equation $G_n = P^z$, Proceedings EUROCAL' 85, Linz, Austria, Vol2, Lecture Notes in Comput. Sci. 204, Springer Verlag, Berlin (1985), 503－512

[92]Pethö, A. and Schulenberg, R., Effektives Lösen von Thue Gleichungen, Publ. Math. Debrecen 34 (1987), 189－196

[93] Pethö, A. and de Weger, B. M. M., Products of prime powers in binary recurrence sequences I: The hyperbolic case, with an application to the generalized Ramanujan – Nagell equation, Math. Comp. 47 (1986), 713 – 727

[94] Philippon, P. and Waldschmidt, M., Lower bounds for linear forms in logarithms, New advances in transcendence theory (Proc. Symp. Durham July 1986), A. Baber(ed.), Cambridge University Press, Cambridge (1988), 280 – 312

[95] Pinch, R. G. E., Elliptic curves with good reduction away from 2, Math. Proc. Camb. Phil. Soc. 96(1984), 25 – 38

[96] Pinch, R. G. E., Simultaneous Pellian equations, Math Proc. Camp. Phil. Soc. 103 (1988), 35 – 46

[97] Pohst, M. and Zassenhaus, H., On effective computation of fundamental units I & II, Math. Comp. 38 (1982), 275 – 291 & 293 – 329

[98] Van der Poorten, A. J., Linear forms in logarithms in the p – adic case, transcendence Theory: Advances and Applications, A. Baker(ed.), Academic Press, London (1977), 29 – 57

[99] Ramasamy, A. M. S., Ramanujan's equation, J. Ramanujan Math. Soc. 7 (1992), 133 – 153

[100] Rumsey, H. Jr. and posner, E. C., On a class of exponential equations, Proc. Am. Math. Soc. 15 (1964), 974 – 978)

[101] Schinzel, A., On two theorems of Gelfond and some of

their applications, Acta Arith. 13(1967), 177 – 236

[102] Schmidt, W. M., Diophantine Approximation, Lecture Notes in Math., 785, Springer – Verlag, Berlin, 1980

[103] Schmidt, W. M., The number of solutions of Thue gquations, New advances in transcendence theory (Proc. Symp. Durham July 1986), A. Baker (ed.), Cambridge University Press, Cambridge(1988), 337 – 346

[104] Schmidt, W. M., Diophantine Approximations and Diophantine Equations, Lecture Notesin Math., 1467, Springer – Verlag, Berlin, 1991

[105] Setzer, B., Elliptic curves of prime conductor, J. London Math. Soc. 10[1975], 367 – 378

[106] Shorey, T. N., van der Poorten, A. J., Tijdeman, R. and Schinzel, A., Applications of the Gel′fond – Baker method to diophantine equations, Transcendence Theory: Advances and Applications, A. Baker (ed), Academic Press, London(1977), 59 – 77

[107] Shorey, T. N. and Tijdeman, R., Exponential Diophantine Equations, Cambridge University Press, Cambridge (1986)

[108] Sprindżuk, V. G., Effective estimates in 'ternary' exponential diophantine equations (Russian), Dokl. Akad. Nauk BSSR 12(1969), 293 – 297

[109] Steiner, R. P.; A theorem on the Syracuse problem, Proc. Seventh Manitoba Conf. Numer. Math. Comp. (1977), 553 – 559

[110]Steiner, R. P., On Mordell's equation $y^2 - k = x^3$: a problem of Stolarsky, Math Comp. 46(1986), 703 – 714

[111] Stewart, C. L. and Tijdeman, R., On the Oesterlé - Massen conjecture, Monatsh. Math. 102 (1986), 251 - 257

[112]Stewart, C. L. and Yu, K. – R., On the abc conjeture, Math. Ann. 291(1991), 225 – 230

[113]StØrmer, C., Quelques théorémes sur l'équation de Pell $x^2 - Dy^2 = \pm 1$ et leurs applications, Vid. Skr. I Math. Natur. Kl. (Christiana), No. 2(1897)

[114]Stroeker, R. J. and Tijdeman, R., Diophantine equations, (with and Appendixby P. L. Cijsouw, A. korlaar an R. Tijdeman), Computational Methods in Number Theory, H. W. Lenstra and R. Tijdeman(eds.), MC Tract 115, Centr. Math. Comp. Sci., Amsterdam(1982), 321 – 369

[115] Thue, A., Über Annäherungswerten algebraischer Zahlen, J. reine angew. Math. 135(1909), 284 – 305

[116] Tijdeman, R., On integers with many small prime factors, Compositio Math. 26(1973), 319 – 330

[117]Tijdeman, R., On the equation of Catalan, Acta Arith. 29 (1976), 197 – 209

[118]Tijdeman, R., On the Fermat – Catalan equation, Jahresber. Deutsche Math. Verein. 87(1985), 1 – 18

[119]Tijdeman, R., Diophantine equations and diophantine approximations, Proceedings NATO Advanced Study Institube en Number Theory and Applications (Banff, AB,

1988), 215 – 243, NATO AST Ser. C, Reidel, Dordrecht (1989)

[120] Tijdeman, R. and Wang, L., Sums of products of powers of given prime numbers, Pacific J. Math. 132(1988), 177 – 193

[121] Tzanakis, N., On the diophantine equation $y^2 - D = 2^k$, J. Number Theory 17(1983), 144 – 164

[122] Tzanakis, N., The complete solution in integers of $x^3 + 2y^3 = 2^n$, J. Number Theory 19(1984), 203 – 208

[123] Tzanakis, N., On the practical solution of the Thue equation, an outline, Proceedings Colloquium on Number Theory. Vol. II (Budapest, 1987), 1003 – 1012, North Holland, Amsterdam (1990)

[124] Tzanakis, N. and de Weger B. M. M., On the practical solution of the Thue equation, J. Number Theory 31, 99 – 132. Preprint version with numberical details: Memorandum No. 668, Faculty of Applied Mathematics, University of Twente, October 1987 (1989ª)

[125] Tzanakis, N. and de Weger B. M. M., Solving specific Thue – Mahler equation, Math. Comp. 57(1991), 799 – 815

[126] Tzanakis, N. and Wolfskill, J., On the diophantine equt〈tion $y^2 = 4q^n + 4q + 1$, J. Number Theory 23(1986), 219 – 237

[127] Tzanakis, N. and Wolfskill, J., The diophantine eqution $x^2 = 4q^{a/2} + 4q + 1$ with an application in coding theory,

J. Number Theory 26(1987), 96 – 116

[128] Vojta, P., Diophantine Approximations and Value Distribution Theory, Lecture Notes in Mathematics 1239, Springer Verlag, Berlin(1987)

[129] Wagstaff, S. S. Jr., Solution of Nathànson's exponential congruence, Math. Comp. 33(1979), 1097 – 1100

[130] Wagstaff, S. S. Jr., The computational complexity of solving exponential congruences, Congressus Numerantium, University of Winnipeg, Canada, Vol. 31 (1981), 275 – 286

[131] Waldschmidt, M., A lower bound for linear forms in logarithms, Acta Arith. 37(1980), 257 – 283

[132] Waldschmidt, M., Linear Independence of Logarithms of Algebraic Numbers, Matscience lecture Notes, Madras (1992)

[133] Waldschmidt, M., Minorations de combinaisons linéaires de logarithmes de nombres algébriques, Canada J. Math. 45(1993), 176 – 224

[134] de Weger, B. M. M., Approximation lattices of p – adic numbers, J. Number Theory 24(1986[a]), 70 – 88

[135] de Weger, B. M. M., Products of prime powers in binary recurrence sequences II: The elliptic case, with an application to a mixed quadratic – exponential equation, Math. Comp. 47(1986[b]), 729 – 739

[136] de Weger, B. M. M., Solving exponential diophantine equations using lattic basis reduction algorithms, J. Num

ber Theory 26(1987), 325 - 367. Erratum: J. Number Theory 31(1989), 88 - 89

[137]de Weger, B. M. M., On the practiacl solution of Thue - Mahler equations, an outline, Proceedings Colloquium on Number Theory Vol. II(Budapest, 1987), 1037 - 1050, North Holland, Amsterdam(1990)

[138]de Weger, B. M. M., A diophantine equation of Antoniadis, Proceedings NATO Advanced Study Institute on Number Theory and Applications(Banff, AB, 1988), 575 - 589, Reidel, Dordrecht(1989)

[139]de Weger, B. M. M., Algorithms for Diophantine Equations, CWI. Tract, 65, Stichting Mathematisch Centrum, Amsterdam(1989)

[140]Wüstholz, G., A new approach to Baker's theorem on linear forms in logarithms III, New advances in transcendence theory(Proc. Symp. Durham July 1986), A. Baker (ed.), Cambridge University Press, Cambridge(1988), 399 - 410

[141]Y, K. R., Linear forms in the p - adic logarithms, Report MPI/87 - 20, Max planck Institut fur Mathematik, Bonn.,. Acta Arith. (1987)

[142]Y, K. R., Linear forms in logarithms in the p - adic case, New advances in transcendence theory(Proc. Symp. Durbam July 1986), A. Baker(de), Cambridge University Press, Cambridge(1988), 411 - 434

[143]Y, K. R., Linear forms in p - adic logarithms, I: Acta

Arith. 53 (1989), 107 – 186; II: Compositio Math. 74 (1990), 15 – 113; III: Compositio Math. 91 (1994), 241 – 276.

[General Information]
书名=丢番图方程的计算方法
作者=郭永东，薛国芬，李由编著
页数=280
SS号=12795414
DX号=
出版日期=1995.12
出版社=新疆大学出版社